TigerStack 1000

Gigabit Ethernet Switch

- 24/48 auto-MDI/MDI-X 10/100/1000BASE-T ports
- 4 RJ-45 ports shared with 4 SFP transceiver slots
- 1 10GBASE extender module slot
- Non-blocking switching architecture
- Support for a redundant power unit
- Spanning Tree Protocol, RSTP, and MSTP
- Up to 32 LACP or static 8-port trunks
- Layer 2/3/4 CoS support through eight priority queues
- Layer 3/4 traffic priority with IP Precedence and IP DSCP
- Full support for VLANs with GVRP
- IGMP multicast filtering and snooping
- Support for jumbo frames up to 9 KB
- Manageable via console, Web, SNMP/RMON
- Security features: ACL, RADIUS, 802.1x
- Routing features: IP/RIP routing, OSPF, VRRP, CIDR

SMC® Networks

Management Guide

SMC8724ML3
SMC8748ML3

TigerStack 1000 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC® Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

June 2005
Pub. # 149100023600A

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2005 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618
All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at: **http://www.smc.com/index.cfm?action=customer_service_warranty**.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

TABLE OF CONTENTS

1 Introduction 1-1

Key Features 1-1
Description of Software Features 1-3
System Defaults 1-9

2 Initial Configuration 2-1

Connecting to the Switch 2-1
Configuration Options 2-1
Required Connections 2-3
Remote Connections 2-4
Stack Operations 2-5
Selecting the Stack Master 2-5
Selecting the Backup Unit 2-6
Recovering from Stack Failure or Topology Change 2-6
Broken Link for Line and Wrap-around Topologies 2-7
Resilient IP Interface for Management Access 2-7
Resilient Configuration 2-8
Renumbering the Stack 2-8
Basic Configuration 2-8
Console Connection 2-8
Setting Passwords 2-9
Setting an IP Address 2-10
Manual Configuration 2-10
Dynamic Configuration 2-11
Enabling SNMP Management Access 2-12
Community Strings (for SNMP version 1 and 2c clients) . 2-13
Trap Receivers 2-14
Configuring Access for SNMP Version 3 Clients 2-14
Saving Configuration Settings 2-15
Managing System Files 2-16

3 Configuring the Switch 3-1

Using the Web Interface 3-1
Navigating the Web Browser Interface 3-3
Home Page 3-3

Configuration Options 3-4
Panel Display 3-4
Main Menu 3-5
Basic Configuration 3-15
Displaying System Information 3-15
Displaying Switch Hardware/Software Versions 3-17
Displaying Bridge Extension Capabilities 3-19
Configuring Support for Jumbo Frames 3-21
Setting the Switch's IP Address 3-22
Manual Configuration 3-23
Using DHCP/BOOTP 3-25
Managing Firmware 3-27
Downloading System Software from a Server 3-28
Saving or Restoring Configuration Settings 3-30
Downloading Configuration Settings from a Server 3-32
Console Port Settings 3-34
Telnet Settings 3-36
Configuring Event Logging 3-38
System Log Configuration 3-38
Remote Log Configuration 3-41
Displaying Log Messages 3-43
Sending Simple Mail Transfer Protocol Alerts 3-44
Renumbering the Stack 3-46
Resetting the System 3-47
Setting the System Clock 3-48
Configuring SNTP 3-48
Setting the Time Zone 3-49
Simple Network Management Protocol 3-50
Enabling the SNMP Agent 3-53
Setting Community Access Strings 3-53
Specifying Trap Managers and Trap Types 3-54
Configuring SNMPv3 Management Access 3-58
Setting an Engine ID 3-58
Specifying a Remote Engine ID 3-59
Configuring SNMPv3 Users 3-60
Configuring Remote SNMPv3 Users 3-63
Configuring SNMPv3 Groups 3-66

Setting SNMPv3 Views 3-72
User Authentication 3-74
Configuring User Accounts 3-75
Configuring Local/Remote Logon Authentication 3-76
Configuring HTTPS 3-80
Replacing the Default Secure-site Certificate 3-82
Configuring the Secure Shell 3-83
Generating the Host Key Pair 3-86
Configuring the SSH Server 3-88
Configuring Port Security 3-90
Configuring 802.1X Port Authentication 3-93
Displaying 802.1X Global Settings 3-94
Configuring 802.1X Global Settings 3-95
Configuring Port Settings for 802.1X 3-96
Displaying 802.1X Statistics 3-99
Filtering IP Addresses for Management Access 3-101
Access Control Lists 3-103
Configuring Access Control Lists 3-103
Setting the ACL Name and Type 3-104
Configuring a Standard IP ACL 3-105
Configuring an Extended IP ACL 3-106
Configuring a MAC ACL 3-109
Configuring ACL Masks 3-111
Specifying the Mask Type 3-112
Configuring an IP ACL Mask 3-113
Configuring a MAC ACL Mask 3-115
Binding a Port to an Access Control List 3-117
Port Configuration 3-119
Displaying Connection Status 3-119
Configuring Interface Connections 3-122
Creating Trunk Groups 3-125
Statically Configuring a Trunk 3-126
Enabling LACP on Selected Ports 3-128
Configuring LACP Parameters 3-130
Displaying LACP Port Counters 3-134
Displaying LACP Settings and Status for the Local Side 3-135
Displaying LACP Settings and Status for Remote Side . 3-138

Setting Broadcast Storm Thresholds 3-140
Configuring Port Mirroring 3-142
Configuring Rate Limits 3-144
Showing Port Statistics 3-145
Address Table Settings 3-151
Setting Static Addresses 3-151
Displaying the Address Table 3-153
Changing the Aging Time 3-155
Spanning Tree Algorithm Configuration 3-155
Displaying Global Settings 3-157
Configuring Global Settings 3-161
Displaying Interface Settings 3-166
Configuring Interface Settings 3-170
Configuring Multiple Spanning Trees 3-173
Displaying Interface Settings for MSTP 3-177
Configuring Interface Settings for MSTP 3-179
VLAN Configuration 3-181
IEEE 802.1Q VLANs 3-181
Enabling or Disabling GVRP (Global Setting) 3-185
Displaying Basic VLAN Information 3-186
Displaying Current VLANs 3-187
Creating VLANs 3-188
Adding Static Members to VLANs (VLAN Index) 3-190
Adding Static Members to VLANs (Port Index) 3-193
Configuring VLAN Behavior for Interfaces 3-194
Configuring Private VLANs 3-197
Enabling Private VLANs 3-197
Configuring Uplink and Downlink Ports 3-198
Configuring Protocol-Based VLANs 3-199
Configuring Protocol Groups 3-200
Mapping Protocols to VLANs 3-201
Class of Service Configuration 3-203
Layer 2 Queue Settings 3-203
Setting the Default Priority for Interfaces 3-203
Mapping CoS Values to Egress Queues 3-205
Selecting the Queue Mode 3-207
Setting the Service Weight for Traffic Classes 3-208

Layer 3/4 Priority Settings 3-209
Mapping Layer 3/4 Priorities to CoS Values 3-209
Selecting IP Precedence/DSCP Priority 3-210
Mapping IP Precedence 3-210
Mapping DSCP Priority 3-212
Mapping IP Port Priority 3-214
Quality of Service 3-216
Configuring Quality of Service Parameters 3-217
Configuring a Class Map 3-218
Creating QoS Policies 3-221
Attaching a Policy Map to Ingress Queues 3-225
Multicast Filtering 3-226
Layer 2 IGMP (Snooping and Query) 3-227
Configuring IGMP Snooping and Query Parameters . . . 3-228
Displaying Interfaces Attached to a Multicast Router . . . 3-230
Specifying Static Interfaces for a Multicast Router 3-231
Displaying Port Members of Multicast Services 3-232
Assigning Ports to Multicast Services 3-233
Configuring Domain Name Service 3-235
Configuring General DNS Server Parameters 3-235
Configuring Static DNS Host to Address Entries 3-238
Displaying the DNS Cache 3-240
Dynamic Host Configuration Protocol 3-242
Configuring DHCP Relay Service 3-242
Configuring the DHCP Server 3-244
Enabling the Server, Setting Excluded Addresses 3-245
Configuring Address Pools 3-246
Displaying Address Bindings 3-252
Configuring Router Redundancy 3-254
Virtual Router Redundancy Protocol 3-256
Configuring VRRP Groups 3-256
Displaying VRRP Global Statistics 3-262
Displaying VRRP Group Statistics 3-263
IP Routing 3-265
Overview 3-265
Initial Configuration 3-265

IP Switching 3-266
Routing Path Management 3-268
Routing Protocols 3-268
Basic IP Interface Configuration 3-269
Configuring IP Routing Interfaces 3-271
Address Resolution Protocol 3-273
Proxy ARP 3-274
Basic ARP Configuration 3-274
Configuring Static ARP Addresses 3-276
Displaying Dynamically Learned ARP Entries 3-277
Displaying Local ARP Entries 3-279
Displaying ARP Statistics 3-280
Displaying Statistics for IP Protocols 3-282
IP Statistics 3-282
ICMP Statistics 3-284
UDP Statistics 3-287
TCP Statistics 3-288
Configuring Static Routes 3-289
Displaying the Routing Table 3-290
Configuring the Routing Information Protocol 3-292
Configuring General Protocol Settings 3-293
Specifying Network Interfaces for RIP 3-295
Configuring Network Interfaces for RIP 3-296
Displaying RIP Information and Statistics 3-300
Configuring the Open Shortest Path First Protocol 3-303
Configuring General Protocol Settings 3-305
Configuring OSPF Areas 3-309
Configuring Area Ranges
(Route Summarization for ABRs) 3-313
Configuring OSPF Interfaces 3-315
Configuring Virtual Links 3-321
Configuring Network Area Addresses 3-323
Configuring Summary Addresses
(for External AS Routes) 3-325
Redistributing External Routes 3-327
Configuring NSSA Settings 3-329
Displaying Link State Database Information 3-330

Displaying Information on Border Routers 3-333
Displaying Information on Neighbor Routers 3-334

4 Command Line Interface 4-1

Using the Command Line Interface 4-1
Accessing the CLI 4-1
Console Connection 4-1
Telnet Connection 4-2
Entering Commands 4-3
Keywords and Arguments 4-3
Minimum Abbreviation 4-4
Command Completion 4-4
Getting Help on Commands 4-4
Showing Commands 4-4
Partial Keyword Lookup 4-6
Negating the Effect of Commands 4-6
Using Command History 4-6
Understanding Command Modes 4-7
Exec Commands 4-7
Configuration Commands 4-8
Command Line Processing 4-11
Command Groups 4-12
Line Commands 4-14
line 4-15
login 4-16
password 4-17
timeout login response 4-18
exec-timeout 4-19
password-thresh 4-20
silent-time 4-21
databits 4-21
parity 4-22
speed 4-23
stopbits 4-24
disconnect 4-24
show line 4-25

General Commands 4-26
enable 4-27
disable 4-28
configure 4-28
show history 4-29
reload 4-30
end 4-30
exit 4-31
quit 4-31
System Management Commands 4-32
Device Designation Commands 4-33
prompt 4-33
hostname 4-34
switch renumber 4-34
User Access Commands 4-35
username 4-35
enable password 4-37
IP Filter Commands 4-38
management 4-38
show management 4-39
Web Server Commands 4-40
ip http port 4-41
ip http server 4-41
ip http secure-server 4-42
ip http secure-port 4-43
Telnet Server Commands 4-44
ip telnet server 4-44
Secure Shell Commands 4-45
ip ssh server 4-48
ip ssh timeout 4-49
ip ssh authentication-retries 4-50
ip ssh server-key size 4-51
delete public-key 4-51
ip ssh crypto host-key generate 4-52
ip ssh crypto zeroize 4-53
ip ssh save host-key 4-54
show ip ssh 4-54

show ssh 4-55
show public-key 4-56
Event Logging Commands 4-57
logging on 4-58
logging history 4-58
logging host 4-60
logging facility 4-60
logging trap 4-61
clear log 4-62
show logging 4-62
show log 4-64
SMTP Alert Commands 4-65
logging sendmail host 4-65
logging sendmail level 4-66
logging sendmail source-email 4-67
logging sendmail destination-email 4-68
logging sendmail 4-68
show logging sendmail 4-69
Time Commands 4-69
sntp client 4-70
sntp server 4-71
sntp poll 4-72
show sntp 4-73
clock timezone 4-73
calendar set 4-74
show calendar 4-75
System Status Commands 4-75
show startup-config 4-76
show running-config 4-78
show system 4-80
show users 4-81
show version 4-81
Frame Size Commands 4-82
jumbo frame 4-82
Flash/File Commands 4-83
copy 4-84
delete 4-87

dir 4-88
whichboot 4-89
boot system 4-90
Authentication Commands 4-91
Authentication Sequence 4-91
authentication login 4-92
authentication enable 4-93
RADIUS Client 4-94
radius-server host 4-95
radius-server port 4-96
radius-server key 4-96
radius-server retransmit 4-97
radius-server timeout 4-97
show radius-server 4-98
TACACS+ Client 4-99
tacacs-server host 4-99
tacacs-server port 4-100
tacacs-server key 4-100
show tacacs-server 4-101
Port Security Commands 4-101
port security 4-102
802.1X Port Authentication 4-104
dot1x system-auth-control 4-105
dot1x default 4-105
dot1x max-req 4-105
dot1x port-control 4-106
dot1x operation-mode 4-107
dot1x re-authenticate 4-108
dot1x re-authentication 4-108
dot1x timeout quiet-period 4-109
dot1x timeout re-authperiod 4-109
dot1x timeout tx-period 4-110
show dot1x 4-110
Access Control List Commands 4-114
IP ACLs 4-116
access-list ip 4-117
permit, deny (Standard ACL) 4-118

permit, deny (Extended ACL) 4-119
show ip access-list 4-121
access-list ip mask-precedence 4-122
mask (IP ACL) 4-123
show access-list ip mask-precedence 4-126
ip access-group 4-127
show ip access-group 4-128
MAC ACLs 4-128
access-list mac 4-129
permit, deny (MAC ACL) 4-130
show mac access-list 4-132
access-list mac mask-precedence 4-132
mask (MAC ACL) 4-133
show access-list mac mask-precedence 4-135
mac access-group 4-136
show mac access-group 4-137
ACL Information 4-137
show access-list 4-137
show access-group 4-138
SNMP Commands 4-139
snmp-server 4-140
show snmp 4-140
snmp-server community 4-141
snmp-server contact 4-142
snmp-server location 4-143
snmp-server host 4-143
snmp-server enable traps 4-146
snmp-server engine-id 4-147
show snmp engine-id 4-149
snmp-server view 4-150
show snmp view 4-151
snmp-server group 4-152
show snmp group 4-153
snmp-server user 4-154
show snmp user 4-156

DHCP Commands 4-157
DHCP Client 4-157
ip dhcp client-identifier 4-157
ip dhcp restart client 4-158
DHCP Relay 4-159
ip dhcp restart relay 4-159
ip dhcp relay server 4-160
DHCP Server 4-161
service dhcp 4-162
ip dhcp excluded-address 4-163
ip dhcp pool 4-163
network 4-164
default-router 4-165
domain-name 4-166
dns-server 4-167
next-server 4-167
bootfile 4-168
netbios-name-server 4-169
netbios-node-type 4-170
lease 4-171
host 4-172
client-identifier 4-173
hardware-address 4-174
clear ip dhcp binding 4-175
show ip dhcp binding 4-176
DNS Commands 4-177
ip host 4-178
clear host 4-179
ip domain-name 4-179
ip domain-list 4-180
ip name-server 4-181
ip domain-lookup 4-182
show hosts 4-183
show dns 4-184
show dns cache 4-184
clear dns cache 4-185

Interface Commands 4-186
interface 4-187
description 4-187
speed-duplex 4-188
negotiation 4-189
capabilities 4-190
media-type 4-192
shutdown 4-193
switchport broadcast packet-rate 4-194
clear counters 4-195
show interfaces status 4-196
show interfaces counters 4-197
show interfaces switchport 4-199
Mirror Port Commands 4-200
port monitor 4-201
show port monitor 4-202
Rate Limit Commands 4-203
rate-limit 4-203
Link Aggregation Commands 4-204
channel-group 4-206
lacp 4-206
lacp system-priority 4-208
lacp admin-key (Ethernet Interface) 4-209
lacp admin-key (Port Channel) 4-210
lacp port-priority 4-211
show lacp 4-212
Address Table Commands 4-216
mac-address-table static 4-217
clear mac-address-table dynamic 4-218
show mac-address-table 4-219
mac-address-table aging-time 4-220
show mac-address-table aging-time 4-220
Spanning Tree Commands 4-221
spanning-tree 4-222
spanning-tree mode 4-223
spanning-tree forward-time 4-225
spanning-tree hello-time 4-226

spanning-tree max-age 4-226
spanning-tree priority 4-227
spanning-tree pathcost method 4-228
spanning-tree transmission-limit 4-229
spanning-tree mst-configuration 4-229
mst vlan 4-230
mst priority 4-231
name 4-232
revision 4-233
max-hops 4-233
spanning-tree spanning-disabled 4-234
spanning-tree cost 4-235
spanning-tree port-priority 4-236
spanning-tree edge-port 4-237
spanning-tree portfast 4-238
spanning-tree link-type 4-239
spanning-tree mst cost 4-240
spanning-tree mst port-priority 4-241
spanning-tree protocol-migration 4-242
show spanning-tree 4-243
show spanning-tree mst configuration 4-245
VLAN Commands 4-245
Editing VLAN Groups 4-246
vlan database 4-246
vlan 4-247
Configuring VLAN Interfaces 4-248
interface vlan 4-249
switchport mode 4-250
switchport acceptable-frame-types 4-251
switchport ingress-filtering 4-252
switchport native vlan 4-253
switchport allowed vlan 4-254
switchport forbidden vlan 4-255
Displaying VLAN Information 4-256
show vlan 4-256
Configuring Private VLANs 4-257
pvlan 4-257

show pvlan 4-258
Configuring Protocol-based VLANs 4-259
protocol-vlan protocol-group (Configuring Groups) . . . 4-260
protocol-vlan protocol-group (Configuring Interfaces) . 4-261
show protocol-vlan protocol-group 4-262
show interfaces protocol-vlan protocol-group 4-263
GVRP and Bridge Extension Commands 4-264
bridge-ext gvrp 4-264
show bridge-ext 4-265
switchport gvrp 4-266
show gvrp configuration 4-266
garp timer 4-267
show garp timer 4-268
Priority Commands 4-269
Priority Commands (Layer 2) 4-269
queue mode 4-270
switchport priority default 4-271
queue bandwidth 4-272
queue cos-map 4-273
show queue mode 4-274
show queue bandwidth 4-275
show queue cos-map 4-275
Priority Commands (Layer 3 and 4) 4-276
map ip port (Global Configuration) 4-276
map ip port (Interface Configuration) 4-277
map ip precedence (Global Configuration) 4-278
map ip precedence (Interface Configuration) 4-278
map ip dscp (Global Configuration) 4-279
map ip dscp (Interface Configuration) 4-280
show map ip port 4-281
show map ip precedence 4-282
show map ip dscp 4-283
Quality of Service Commands 4-284
class-map 4-286
match 4-287
policy-map 4-289
class 4-290

set 4-291
police 4-292
service-policy 4-293
show class-map 4-294
show policy-map 4-294
show policy-map interface 4-295
Multicast Filtering Commands 4-296
IGMP Snooping Commands 4-296
ip igmp snooping 4-297
ip igmp snooping vlan static 4-297
ip igmp snooping version 4-298
show ip igmp snooping 4-299
show mac-address-table multicast 4-299
IGMP Query Commands (Layer 2) 4-300
ip igmp snooping querier 4-301
ip igmp snooping query-count 4-301
ip igmp snooping query-interval 4-302
ip igmp snooping query-max-response-time 4-303
ip igmp snooping router-port-expire-time 4-304
Static Multicast Routing Commands 4-305
ip igmp snooping vlan mrouter 4-305
show ip igmp snooping mrouter 4-306
IP Interface Commands 4-307
Basic IP Configuration 4-307
ip address 4-308
ip default-gateway 4-310
show ip interface 4-311
show ip redirects 4-311
ping 4-312
Address Resolution Protocol (ARP) 4-313
arp 4-314
arp-timeout 4-315
clear arp-cache 4-315
show arp 4-316
ip proxy-arp 4-316

IP Routing Commands 4-317
Global Routing Configuration 4-318
ip routing 4-318
ip route 4-319
clear ip route 4-320
show ip route 4-320
show ip host-route 4-322
show ip traffic 4-323
Routing Information Protocol (RIP) 4-324
router rip 4-325
timers basic 4-325
network 4-327
neighbor 4-328
version 4-328
ip rip receive version 4-330
ip rip send version 4-331
ip split-horizon 4-332
ip rip authentication key 4-333
ip rip authentication mode 4-334
show rip globals 4-335
show ip rip 4-336
Open Shortest Path First (OSPF) 4-338
router ospf 4-340
router-id 4-340
compatible rfc1583 4-341
default-information originate 4-342
timers spf 4-343
area range 4-344
area default-cost 4-345
summary-address 4-346
redistribute 4-347
network area 4-348
area stub 4-350
area nssa 4-351
area virtual-link 4-353
ip ospf authentication 4-356
ip ospf authentication-key 4-357

ip ospf message-digest-key 4-358
ip ospf cost 4-359
ip ospf dead-interval 4-360
ip ospf hello-interval 4-361
ip ospf priority 4-361
ip ospf retransmit-interval 4-362
ip ospf transmit-delay 4-363
show ip ospf 4-364
show ip ospf border-routers 4-365
show ip ospf database 4-366
show ip ospf interface 4-375
show ip ospf neighbor 4-376
show ip ospf summary-address 4-377
show ip ospf virtual-links 4-378
Multicast Routing Commands 4-379
Static Multicast Routing Commands 4-379
ip igmp snooping vlan mrouter 4-379
show ip igmp snooping mrouter 4-380
Router Redundancy Commands 4-381
Virtual Router Redundancy Protocol Commands 4-381
vrrp ip 4-382
vrrp authentication 4-383
vrrp priority 4-384
vrrp timers advertise 4-385
vrrp preempt 4-386
show vrrp 4-387
show vrrp interface 4-389
show vrrp router counters 4-390
show vrrp interface counters 4-391
clear vrrp router counters 4-391
clear vrrp interface counters 4-392

APPENDICES:

A Software Specifications A-1

Software Features A-1
Management Features A-3
Standards A-3
Management Information Bases A-4

B Troubleshooting B-1

Problems Accessing the Management Interface B-1
Using System Logs B-3

Glossary

Index

TABLES

Table 1-1. Key Features 1-1
Table 1-2 System Defaults 1-9
Table 3-1 Web Page Configuration Buttons 3-4
Table 3-2 Switch Main Menu 3-5
Table 3-3 Logging Levels 3-39
Table 3-4. SNMPv3 Security Models and Levels 3-52
Table 3-5 Supported Notification Messages 3-67
Table 3-6 HTTPS System Support 3-81
Table 3-7 802.1X Statistics 3-99
Table 3-8 LACP Port Counters 3-134
Table 3-9 LACP Internal Configuration Information 3-135
Table 3-10 LACP Neighbor Configuration Information 3-138
Table 3-11 Port Statistics 3-146
Table 3-12 Mapping CoS Values to Egress Queues 3-205
Table 3-13 CoS Priority Levels 3-205
Table 3-14 Mapping IP Precedence 3-211
Table 3-15 Mapping DSCP Priority 3-213
Table 3-16 Address Resolution Protocol 3-273
Table 3-17 ARP Statistics 3-280
Table 3-18 IP Statistics 3-282
Table 3-19 ICMP Statistics 3-285
Table 3-20 USP Statistics 3-287
Table 3-21 TCP Statistics 3-288
Table 3-22 RIP Information and Statistics 3-301
Table 4-1 General Command Modes 4-7
Table 4-2 Configuration Command Modes 4-10
Table 4-3 Keystroke Commands 4-11
Table 4-4 Command Group Index 4-12
Table 4-5 Line Commands 4-14
Table 4-6 General Commands 4-26
Table 4-7 System Management Commands 4-32
Table 4-8 Device Designation Commands 4-33
Table 4-9 User Access Commands 4-35
Table 4-10 Default Login Settings 4-36
Table 4-11 IP Filter Commands 4-38
Table 4-12 Web Server Commands 4-40

Table 4-13 HTTPS System Support 4-43
Table 4-14 Telnet Server Commands 4-44
Table 4-15 Secure Shell Commands 4-46
Table 4-16 show ssh - display description 4-55
Table 4-17 Event Logging Commands 4-57
Table 4-18 Logging Levels 4-59
Table 4-19 show logging flash/ram - display description 4-63
Table 4-20 show logging trap - display description 4-64
Table 4-21 SMTP Alert Commands 4-65
Table 4-22 Time Commands 4-69
Table 4-23 System Status Commands 4-75
Table 4-24 Frame Size Commands 4-82
Table 4-25 Flash/File Commands 4-83
Table 4-26 File Directory Information 4-88
Table 4-27 Authentication Commands 4-91
Table 4-28 Authentication Sequence Commands 4-91
Table 4-29 RADIUS Client Commands 4-94
Table 4-30 TACACS+ Client Commands 4-99
Table 4-31 Port Security Commands 4-102
Table 4-32 802.1X Port Authentication Commands 4-104
Table 4-33 Access Control List Commands 4-116
Table 4-34 IP ACL Commands 4-116
Table 4-35 MAC ACL Commands 4-128
Table 4-36 ACL Information Commands 4-137
Table 4-37 SNMP Commands 4-139
Table 4-38 show snmp engine-id - display description 4-149
Table 4-39 show snmp view - display description 4-151
Table 4-40 show snmp group - display description 4-154
Table 4-41 show snmp user - display description 4-156
Table 4-42 DHCP Commands 4-157
Table 4-43 DHCP Client Commands 4-157
Table 4-44 DHCP Relay Commands 4-159
Table 4-45 DHCP Server Commands 4-161
Table 4-46 DNS Commands 4-177
Table 4-47 show dns cache - display description 4-185
Table 4-48 Interface Commands 4-186
Table 4-50 Mirror Port Commands 4-200

Table 4-49 show interfaces switchport - display description 4-200
Table 4-51 Rate Limit Commands 4-203
Table 4-52 Link Aggregation Commands 4-204
Table 4-53 show lacp counters - display description 4-212
Table 4-54 show lacp internal - display description 4-213
Table 4-55 show lacp neighbors - display description 4-215
Table 4-57 Address Table Commands 4-216
Table 4-56 show lacp sysid - display description 4-216
Table 4-58 Spanning Tree Commands 4-221
Table 4-59 VLAN Commands 4-245
Table 4-60 Editing VLAN Groups 4-246
Table 4-61 Configuring VLAN Interfaces 4-248
Table 4-62 Displaying VLAN Information 4-256
Table 4-63 Private VLAN Commands 4-257
Table 4-64 Protocol-based VLAN Commands 4-259
Table 4-65 GVRP and Bridge Extension Commands 4-264
Table 4-66 Priority Commands 4-269
Table 4-67 Priority Commands (Layer 2) 4-269
Table 4-68 Default CoS Priority Levels 4-273
Table 4-69 Priority Commands (Layer 3 and 4) 4-276
Table 4-70 Mapping IP Precedence to CoS Values 4-279
Table 4-71 Mapping IP DSCP to CoS Values 4-280
Table 4-72 Quality of Service Commands 4-284
Table 4-73 Multicast Filtering Commands 4-296
Table 4-74 IGMP Snooping Commands 4-296
Table 4-75 IGMP Query Commands (Layer 2) 4-300
Table 4-76 Static Multicast Routing Commands 4-305
Table 4-77 IP Interface Commands 4-307
Table 4-78 Basic IP Configuration Commands 4-307
Table 4-79 Address Resolution Protocol Commands 4-313
Table 4-80 IP Routing Commands 4-317
Table 4-81 Global Routing Configuration Commands 4-318
Table 4-82 show ip route - display description 4-321
Table 4-83 show ip host-route - display description 4-322
Table 4-84 Routing Information Protocol Commands 4-324
Table 4-85 show rip globals - display description 4-335
Table 4-86 show ip rip - display description 4-337

Table 4-87 Open Shortest Path First Commands 4-338
Table 4-88 show ip ospf - display description 4-364
Table 4-89 show ip ospf border-routers - display description 4-365
Table 4-90 show ip ospf database - display description 4-367
Table 4-91 show ip ospf asbr-summary - display description 4-368
Table 4-92 show ip ospf database-summary - display description . 4-369
Table 4-93 show ip ospf external - display description 4-370
Table 4-94 show ip ospf network - display description 4-371
Table 4-95 show ip ospf router - display description 4-373
Table 4-96 show ip ospf summary - display description 4-374
Table 4-97 show ip ospf interface - display description 4-375
Table 4-98 show ip ospf neighbor - display description 4-377
Table 4-99 show ip ospf virtual-links - display description 4-378
Table 4-100 Static Multicast Routing Commands 4-379
Table 4-101 Router Redundancy Commands 4-381
Table 4-102 VRRP Commands 4-381
Table 4-103 show vrrp - display description 4-388
Table 4-104 show vrrp brief - display description 4-389
Table B-1 Troubleshooting Chart B-1

FIGURES

Figure 3-1 Home Page 3-3
Figure 3-2 Front Panel Indicators 3-4
Figure 3-3 System Information 3-16
Figure 3-4 Switch Information 3-18
Figure 3-5 Displaying Bridge Extension Configuration 3-20
Figure 3-6 Configuring Support for Jumbo Frames 3-21
Figure 3-7 IP Interface Configuration - Manual 3-23
Figure 3-8 Default Gateway 3-24
Figure 3-9 IP Interface Configuration - DHCP 3-25
Figure 3-10 Copy Firmware 3-28
Figure 3-11 Setting the Startup Code 3-29
Figure 3-12 Deleting Files 3-29
Figure 3-13 Downloading Configuration Settings for Start-Up 3-32
Figure 3-14 Setting the Startup Configuration Settings 3-33
Figure 3-15 Configuring the Console Port 3-35
Figure 3-16 Configuring the Telnet Interface 3-37
Figure 3-17 System Logs 3-40
Figure 3-18 Remote Logs 3-42
Figure 3-19 Displaying Logs 3-43
Figure 3-20 Enabling and Configuring SMTP Alerts 3-45
Figure 3-21 Renumbering the Stack 3-47
Figure 3-22 Resetting the System 3-47
Figure 3-23 SNTP Configuration 3-49
Figure 3-24 Clock Time Zone 3-50
Figure 3-25 Enabling the SNMP Agent 3-53
Figure 3-26 Configuring SNMP Community Strings 3-54
Figure 3-27 Configuring SNMP Trap Managers 3-57
Figure 3-28 Setting the SNMPv3 Engine ID 3-59
Figure 3-29 Setting an Engine ID 3-60
Figure 3-30 Configuring SNMPv3 Users 3-62
Figure 3-31 Configuring Remote SNMPv3 Users 3-65
Figure 3-32 Configuring SNMPv3 Groups 3-71
Figure 3-33 Configuring SNMPv3 Views 3-73
Figure 3-34 User Accounts 3-76
Figure 3-35 Authentication Server Settings 3-79
Figure 3-36 HTTPS Settings 3-82

Figure 3-37 SSH Host-Key Settings 3-87
Figure 3-38 SSH Server Settings 3-89
Figure 3-39 Port Security 3-92
Figure 3-40 802.1X Global Information 3-94
Figure 3-41 802.1X Global Configuration 3-95
Figure 3-42 802.1X Port Configuration 3-97
Figure 3-43 802.1X Port Statistics 3-100
Figure 3-44 IP Filter 3-102
Figure 3-45 Selecting ACL Type 3-105
Figure 3-46 ACL Configuration - Standard IP 3-106
Figure 3-47 ACL Configuration - Extended IP 3-108
Figure 3-48 ACL Configuration - MAC 3-110
Figure 3-49 Selecting ACL Mask Types 3-112
Figure 3-50 ACL Mask Configuration - IP 3-114
Figure 3-51 ACL Mask Configuration - MAC 3-116
Figure 3-52 ACL Port Binding 3-118
Figure 3-53 Port - Port Information 3-120
Figure 3-54 Port - Port Configuration 3-124
Figure 3-55 Static Trunk Configuration 3-127
Figure 3-56 LACP Trunk Configuration 3-129
Figure 3-57 LACP - Aggregation Port 3-132
Figure 3-58 LACP - Port Counters Information 3-134
Figure 3-59 LACP - Port Internal Information 3-137
Figure 3-60 LACP - Port Neighbors Information 3-139
Figure 3-61 Port Broadcast Control 3-141
Figure 3-62 Mirror Port Configuration 3-143
Figure 3-63 Rate Limit Configuration 3-145
Figure 3-64 Port Statistics 3-150
Figure 3-65 Static Addresses 3-152
Figure 3-66 Dynamic Addresses 3-154
Figure 3-67 Address Aging 3-155
Figure 3-68 STA Information 3-160
Figure 3-69 STA Global Configuration 3-165
Figure 3-70 STA Port Information 3-169
Figure 3-71 STA Port Configuration 3-173
Figure 3-72 MSTP VLAN Configuration 3-175
Figure 3-73 MSTP Port Information 3-177

Figure 3-74 MSTP Port Configuration 3-180
Figure 3-75 Globally Enabling GVRP 3-185
Figure 3-76 VLAN Basic Information 3-186
Figure 3-77 VLAN Current Table 3-187
Figure 3-78 VLAN Static List - Creating VLANs 3-189
Figure 3-79 VLAN Static Table - Adding Static Members 3-192
Figure 3-80 VLAN Static Membership by Port 3-193
Figure 3-81 VLAN Port Configuration 3-196
Figure 3-82 Private VLAN Status 3-197
Figure 3-83 Private VLAN Link Status 3-198
Figure 3-84 Protocol VLAN Configuration 3-200
Figure 3-85 Protocol VLAN Port Configuration 3-202
Figure 3-86 Default Port Priority 3-204
Figure 3-87 Traffic Classes 3-206
Figure 3-88 Queue Mode 3-207
Figure 3-89 Queue Scheduling 3-208
Figure 3-90 IP Precedence/DSCP Priority Status 3-210
Figure 3-91 IP Precedence Priority 3-211
Figure 3-92 IP DSCP Priority 3-213
Figure 3-93 IP Port Priority Status 3-215
Figure 3-94 IP Port Priority 3-215
Figure 3-95 Configuring Class Maps 3-220
Figure 3-96 Configuring Policy Maps 3-224
Figure 3-97 Service Policy Settings 3-226
Figure 3-98 IGMP Configuration 3-229
Figure 3-99 Multicast Router Port Information 3-231
Figure 3-100 Static Multicast Router Port Configuration 3-232
Figure 3-101 IP Multicast Registration Table 3-233
Figure 3-102 IGMP Member Port Table 3-234
Figure 3-103 DNS General Configuration 3-237
Figure 3-104 DNS Static Host Table 3-239
Figure 3-105 DNS Cache 3-241
Figure 3-106 DHCP Relay Configuration 3-243
Figure 3-107 DHCP Server General Configuration 3-245
Figure 3-108 DHCP Server Pool Configuration 3-248
Figure 3-109 DHCP Server Pool - Network Configuration 3-249
Figure 3-110 DHCP Server Pool - Host Configuration 3-251

Figure 3-111 DHCP Server - IP Binding 3-253
Figure 3-112 VRRP Group Configuration 3-260
Figure 3-113 VRRP Group Configuration Detail 3-261
Figure 3-114 VRRP Global Statistics 3-263
Figure 3-115 VRRP Group Statistics 3-264
Figure 3-116 IP Global Settings 3-270
Figure 3-117 IP Routing Interface 3-272
Figure 3-118 ARP General 3-275
Figure 3-119 ARP Static Addresses 3-277
Figure 3-120 ARP Dynamic Addresses 3-278
Figure 3-121 ARP Other Addresses 3-279
Figure 3-122 ARP Statistics 3-280
Figure 3-123 IP Statistics 3-284
Figure 3-124 ICMP Statistics 3-286
Figure 3-125 UDP Statistics 3-287
Figure 3-126 TCP Statistics 3-289
Figure 3-127 IP Static Routes 3-290
Figure 3-128 IP Routing Table 3-291
Figure 3-129 RIP General Settings 3-294
Figure 3-130 RIP Network Addresses 3-296
Figure 3-131 RIP Interface Settings 3-300
Figure 3-132 RIP Statistics 3-302
Figure 3-133 OSPF General Configuration 3-308
Figure 3-134 OSPF Area Configuration 3-312
Figure 3-135 OSPF Range Configuration 3-314
Figure 3-136 OSPF Interface Configuration 3-319
Figure 3-137 OSPF Interface Configuration - Detailed 3-320
Figure 3-138 OSPF Virtual Link Configuration 3-322
Figure 3-139 OSPF Network Area Address Configuration 3-324
Figure 3-140 OSPF Summary Address Configuration 3-326
Figure 3-141 OSPF Redistribute Configuration 3-328
Figure 3-142 OSPF NSSA Settings 3-330
Figure 3-143 OSPF Link State Database Information 3-332
Figure 3-144 OSPF Border Router Information 3-333
Figure 3-145 OSPF Neighbor Information 3-335

CHAPTER 1
INTRODUCTION

This switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Table 1-1 Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – SSL/HTTPS; Telnet – SSH SNMP v1/2c – Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X, MAC address filtering
Access Control Lists	Supports up to 32 IP or MAC ACLs
DHCP Client, Relay and Server	Supported
DNS Server	Supported
Port Configuration	Speed and duplex mode
Rate Limiting	Input and output rate limiting per port

Table 1-1 Key Features (Continued)

Feature	Description
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 32 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Address Table	Up to 16K MAC addresses in forwarding table, 1024 static MAC addresses; Up to 8K IP entries in ARP cache, 64K IP entries in routing table, 256 static IP routes
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, protocol-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
Qualify of Service	Supports Differentiated Services (DiffServ)
Router Redundancy	Router backup is provided with the Virtual Router Redundancy Protocol (VRRP)
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, and IGMP for Layer 3

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering and routing provides support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication server to verify the client's right to access the network via an authentication server (i.e., RADIUS server).

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by used to improve performance by blocking unnecessary network traffic

or to implement security controls by restricting access to specific network resources or protocols.

DHCP Server and DHCP Relay – A DHCP server is provided to assign IP addresses to host devices. Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.

Port Configuration – You can manually configure the speed and duplex mode used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3-2002 (formerly IEEE 802.3ad) Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 32 trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the SMC8724ML3 and SMC8748ML3 provide 2 MB and 4 MB, respectively, for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Algorithm – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection and recovery by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the

switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using eight priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

IP Routing – The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you

easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.

OSPF – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

Router Redundancy – The Virtual Router Redundancy Protocol (VRRP) uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of this protocol is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Address Resolution Protocol – The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (i.e., hardware) addresses. This switch supports conventional ARP, which locates the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next. You can configure either static or dynamic entries in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.

Quality of Service – Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query at Layer 2 and IGMP at Layer 3 to manage multicast group registration.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 3-32).

The following table lists some of the basic system defaults.

Table 1-2 System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	auto
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control*	Disabled

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled Relay: Disabled Server: Disabled
	DNS	Server: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPF	Disabled
Router Redundancy	VRRP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	IGMP (Layer 3)	Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

*There are interoperability problems between Flow Control and Head-of-Line (HOL) blocking for the switch ASIC; Flow Control is therefore not supported for this switch.

CHAPTER 2
INITIAL CONFIGURATION

Connecting to the Switch

Configuration Options

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address" on page 2-10.

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as HP OpenView.

The switch's web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast traffic
- Configure router redundancy
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 6 static or LACP trunks per switch, up to 32 per stack
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics
- Configure any stack unit through the same IP address

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Note: When configuring a stack, connect to the console port on the Master unit.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
    - Select the appropriate serial port (COM port 1 or COM port 2).
    - Set to any of the following baud rates: 9600, 19200, 38400, 57600, 115200 (Note: Set to 9600 baud if want to view all the system initialization messages.).
    - Set the data format to 8 data bits, 1 stop bit, and no parity.
    - Set flow control to none.
    - Set the emulation mode to VT100.
    - When using HyperTerminal, select Terminal keys, not Windows keys.

Notes: **1.** When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

2. Refer to "Line Commands" on page 4-14 for a complete description of console configuration options.

3. Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 4-12.

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-10.

Notes: **1.** This switch supports four concurrent Telnet/SSH sessions.

2. Each VLAN group can be assigned its own IP interface address (page 2-10). You can manage the stack via any IP interface in the stack. In other words, the Master unit does not have to include an active port member of a VLAN interface used for management access.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any

computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Stack Operations

Up to eight 24-port or 48-port Gigabit switches can be stacked together as described in the *Installation Guide*. One unit in the stack acts as the Master for configuration tasks and firmware upgrade. All of the other units function in Slave mode, but can automatically take over management of the stack if the Master unit fails.

To configure any unit in the stack, first verify the unit number from the front panel of the switch, and then select the appropriate unit number from the web or console management interface.

Selecting the Stack Master

Note the following points about unit numbering:

- When the stack is initially powered on, the Master unit is designated as unit 1 for a ring topology. For a line topology, the stack is simply numbered from top to bottom, with the first unit in the stack designated at unit 1. This unit identification number appears on the Stack Unit ID LED on the front panel of the switch. It can also be selected on the front panel graphic of the web interface, or from the CLI.
- If more than one stack Master is selected using the Master/Slave push button on the switch's front panel, the system will select the unit with the lowest MAC address as the Master.

- If the Master unit fails and another unit takes over control of the stack, the unit numbering will not change.
- If a unit in the stack fails or is removed from the stack, the unit numbers will not change. This means that when you replace a unit in the stack, the original configuration for the failed unit will be restored to the replacement unit.
- If a unit is removed from the stack and later reattached to the stack, it will retain the original unit number obtained during stacking.
- If a unit is removed from the stack, and powered up as a stand-alone unit, it will also retain the original unit number obtained during stacking.

Selecting the Backup Unit

Once the Master unit finishes booting up, the Slave unit with the lowest MAC address will be selected from the stack as the primary backup unit. The stack Master immediately downloads all configuration information to the backup unit, and continues to update the backup unit with information about any subsequent configuration changes made to any unit in the stack. If the Master unit fails or is powered off, the backup unit will take control of the stack without any loss of configuration settings.

The Slave unit with the lowest MAC address is selected as the Backup unit. If you want to ensure a logical fail over to next unit down in the stack, place the Slave unit with the lowest MAC address directly beneath the Master unit in the stack.

Recovering from Stack Failure or Topology Change

When a link or unit in the stack fails, a trap message is sent and a failure event is logged. The stack will be rebooted after any system failure or topology change. It takes two to three minutes to for the stack to reboot. If the Master unit fails, the backup unit will take over operations as the new Master unit, reboot the stack, and then select another backup unit after the stack finishes rebooting. Also note that powering down a unit or inserting

a new unit in the stack will cause the stack to reboot. If a unit is removed from the stack (due to a power down or failure) or a new unit added to the stack, the original unit IDs are not affected after rebooting, and a new unit is assigned the lowest available unit ID.

Broken Link for Line and Wrap-around Topologies

All units in the stack must be connected via stacking cable. You can connect the units in a simple cascade configuration from the top to the bottom unit. Using this kind of line topology, if any link or unit in the stack fails, the stack will be broken in two. The Stack Link LED on the unit that is no longer receiving traffic from the next unit up or down in the stack will begin flashing to indicate that the stack link is broken.

When the stack fails, a Master unit is selected from the two stack segments, either the unit with the Master button depressed, or the unit with the lowest MAC address if the Master button is not depressed on any unit. The stack reboots and resumes operations. However, note that the IP address will be the same for any common VLANs (with active port connections) that appear in both of the new stack segments. To resolve the conflicting IP addresses, you should manually replace the failed link or unit as soon as possible. If you are using a wrap-around stack topology, a single point of failure in the stack will not cause the stack to fail. It would take two or more points of failure to break the stack apart.

Note: If a stack breaks apart, the IP address will be the same for any common VLANs (with active port connections) that appear in both stack segments.

Resilient IP Interface for Management Access

The stack functions as one integral system for management and configuration purposes. You can therefore manage the stack through any IP interface configured on the stack. The Master unit does not even have to include an active port member in the VLAN interface used for management access. However, if the unit to which you normally connect for management access fails, and there are no active port members on the

other units within this VLAN interface, then this IP address will no longer be available. To retain a constant IP address for management access across fail over events, you should include port members on several units within the primary VLAN used for stack management.

Resilient Configuration

If a unit in the stack fails, the unit numbers will not change. This means that when you replace a unit in the stack, the original configuration for the failed unit will be restored to the replacement unit. This applies to both the Master and Slave units.

Renumbering the Stack

The startup configuration file maps configuration settings to each switch in the stack based on the unit identification number. If the units are no longer numbered sequentially after several topology changes or failures, you can reset the unit numbers using the "Renumbering" command in the web interface or CLI. Just remember to save the new configuration settings to a startup configuration file prior to powering off the stack Master.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Note: You can only access the console interface through the Master unit in the stack.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log

into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.
2. At the Username prompt, enter "admin."
3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the "username" command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level.
2. Type "configure" and press <Enter>.
3. Type "username guest password 0 *password*," for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type "username admin password 0 *password*," for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

      CLI session with the SMC8748ML3 is opened.
      To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the stack to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the stack's master unit, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment (if routing is not enabled on this switch). Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is obtained via DHCP by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address *ip-address netmask*," where "ip-address" is the switch IP address and "netmask" is the network mask for the network. Press <Enter>.

3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway *gateway*," where "gateway" is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the "bootp" or "dhcp" option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the "ip dhcp restart client" command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the "bootp" or "dhcp" option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
   - To obtain IP settings via DHCP, type "ip address dhcp" and press <Enter>.
   - To obtain IP settings via BOOTP, type "ip address bootp" and press <Enter>.

3. Type “end” to return to the Privileged Exec mode. Press <Enter>.
4. Type “ip dhcp restart client” to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.
6. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart client
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community

string that provides read access to the entire MIB tree, and a default view for the "private" community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see page 3-72).

Community Strings (for SNMP version 1 and 2c clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server community *string mode*," where "string" is the community access string and "mode" is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type "no snmp-server community *string*," where "string" is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the "snmp-server host" command. From the Privileged Exec level global configuration mode prompt, type:

"snmp-server host *host-address community-string*
[version {1 | 2c | 3 {auth | noauth | priv}}]"

where "host-address" is the IP address for the trap receiver, "community-string" specifies access rights for a version 1/2c host, or is the user name of a version 3 host, "version" indicates the SNMP client version, and "auth | noauth | priv" means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host" on page 4-143. The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called "mib-2" that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call "r&d" and specifies group authentication via MD5 or SHA. In

the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password "greenpeace" for authentication, and the password "einstien" for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5
greenpeace priv des56 einstien
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to "Simple Network Management Protocol" on page 3-50, or refer to the specific CLI commands for SNMP starting on page 4-139.

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the "copy" command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. The file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the master unit will also create a file named "startup1.cfg" that contains system settings for stack initialization, including information about the unit identifier, MAC address, and installed module type for each unit the stack. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the stack. See "Saving or Restoring Configuration Settings" on page 3-22 for more information. See "Saving or Restoring Configuration Settings" on page 3-30 for more information.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See "Managing Firmware" on page 3-27 for more information.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

CHAPTER 3
CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4 "Command Line Interface."

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 2-10.)
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 2-9.)
3. After you enter a user name and password, you will have access to the system configuration program.

Notes: **1.** You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

2. If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings" on page 3-170.

Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

Home Page

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

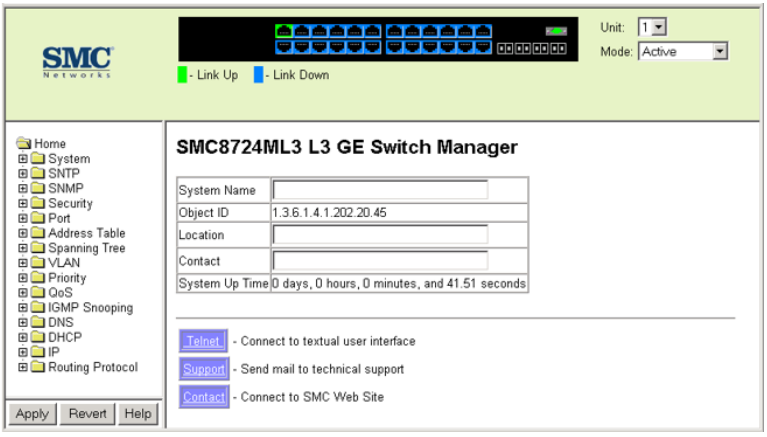


Figure 3-1 Home Page

Note: The examples in this chapter are based on the SMC8724ML3. Other than the number of fixed ports, there are no major differences between the SMC8724ML3 and SMC8748ML3.

Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

Table 3-1 Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
Help	Links directly to web help.

Notes: 1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

Panel Display

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control[1]. Clicking on the image of a port opens the Port Configuration page as described on page 3-122.



Figure 3-2 Front Panel Indicators

1. There are interoperability problems between Flow Control and Head-of-Line (HOL) blocking for the switch ASIC; Flow Control is therefore not supported for this switch.

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 3-2 Switch Main Menu

Menu	Description	Page
System		3-15
System Information	Provides basic system description, including contact information	3-15
Switch Information	Shows the number of ports, hardware/ firmware version numbers, and power status	3-17
Bridge Extension	Shows the bridge extension parameters	3-19
Jumbo Frames	Enables support for jumbo frames	3-21
File Management		3-27
Copy Operation	Allows the transfer and copying files	3-27
Delete	Allows deletion of files from the flash memory	3-27
Set Startup	Sets the startup file	3-27
Line		3-34
Console	Sets console port connection parameters	3-34
Telnet	Sets Telnet connection parameters	3-36
Log		3-38
Logs	Sends error messages to a logging process	3-38
System Logs	Stores and displays error messages	3-43
Remote Logs	Configures the logging of messages to a remote logging process	3-41
SMTP	Sends an SMTP client message to a participating server	3-44
Renumbering	Renumbers the units in the stack	3-46
Reset	Restarts the switch	3-47

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
SNTP		3-48
Configuration	Configures SNTP client settings, including a specified list of servers	3-48
Clock Time Zone	Sets the local time zone for the system clock	3-49
SNMP		3-50
Configuration	Configures community strings and related trap functions	3-53
Agent Status	Enables or disables SNMP	3-53
SNMPv3		3-58
Engine ID	Sets the SNMP v3 engine ID	3-58
Remote Engine ID	Sets the SNMP v3 engine ID on a remote device	3-59
Users	Configures SNMP v3 users	3-60
Remote Users	Configures SNMP v3 users on a remote device	3-63
Groups	Configures SNMP v3 groups	3-66
Views	Configures SNMP v3 views	3-72
Security		3-53
User Accounts	Configures user names, passwords, and access levels	3-75
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	3-76
HTTPS Settings	Configures secure HTTP settings	3-80
SSH		3-83
Settings	Configures Secure Shell server settings	3-88
Host-Key Settings	Generates the host key pair (public and private)	3-86
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	3-90

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
802.1X	Port authentication	3-93
Information	Displays global configuration settings	3-94
Configuration	Configures global configuration parameters	3-95
Port Configuration	Sets the authentication mode for individual ports	3-96
Statistics	Displays protocol statistics for the selected port	3-99
ACL		3-103
Configuration	Configures packet filtering based on IP or MAC addresses	3-103
Mask Configuration	Controls the order in which ACL rules are checked	3-111
Port Binding	Binds a port to the specified ACL	3-117
IP Filter	Configures IP addresses that are allowed management access	3-101
Port		3-119
Port Information	Displays port connection status	3-119
Trunk Information	Displays trunk connection status	3-119
Port Configuration	Configures port connection settings	3-122
Trunk Configuration	Configures trunk connection settings	3-122
Trunk Membership	Specifies ports to group into static trunks	3-126
LACP		3-125
Configuration	Allows ports to dynamically join trunks	3-128
Aggregation Port	Configures parameters for link aggregation group members	3-130
Port Counters Information	Displays statistics for LACP protocol messages	3-134
Port Internal Information	Displays settings and operational state for the local side	3-135

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Port Neighbors Information	Displays settings and operational state for the remote side	3-138
Port Broadcast Control	Sets the broadcast storm threshold for each port	3-140
Trunk Broadcast Control	Sets the broadcast storm threshold for each trunk	3-140
Mirror Port Configuration	Sets the source and target ports for mirroring	3-142
Rate Limit		3-144
Input Port Configuration	Sets the input rate limit for each port	3-144
Input Trunk Configuration	Sets the input rate limit for each trunk	3-144
Output Port Configuration	Sets the output rate limit for each port	3-144
Output Trunk Configuration	Sets the output rate limit for each trunk	3-144
Port Statistics	Lists Ethernet and RMON port statistics	3-145
Address Table		3-151
Static Addresses	Displays entries for interface, address or VLAN	3-151
Dynamic Addresses	Displays or edits static entries in the Address Table	3-153
Address Aging	Sets timeout for dynamically learned entries	3-155
Spanning Tree		3-155
STA		
Information	Displays STA values used for the bridge	3-157
Configuration	Configures global bridge settings for STP, RSTP and MSTP	3-161
Port Information	Displays individual port settings for STA	3-166
Trunk Information	Displays individual trunk settings for STA	3-166

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Port Configuration	Configures individual port settings for STA	3-170
Trunk Configuration	Configures individual trunk settings for STA	3-170
MSTP		
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	3-173
Port Information	Displays port settings for a specified MST instance	3-177
Trunk Information	Displays trunk settings for a specified MST instance	3-177
Port Configuration	Configures port settings for a specified MST instance	3-179
Trunk Configuration	Configures trunk settings for a specified MST instance	3-179
VLAN		3-181
802.1Q VLAN		
GVRP Status	Enables GVRP VLAN registration protocol	3-185
Basic Information	Displays information on the VLAN type supported by this switch	3-186
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	3-187
Static List	Used to create or remove VLAN groups	3-188
Static Table	Modifies the settings for an existing VLAN	3-190
Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden	3-193
Port Configuration	Specifies default PVID and VLAN attributes	3-194
Trunk Configuration	Specifies default trunk VID and VLAN attributes	3-194

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Private VLAN		
Status	Enables or disables the private VLAN	3-197
Link Status	Configures the private VLAN	3-198
Protocol VLAN		
Configuration	Creates a protocol group, specifying the supported protocols	3-200
Port Configuration	Maps a protocol group to a VLAN	3-201
Priority		3-203
Default Port Priority	Sets the default priority for each port	3-203
Default Trunk Priority	Sets the default priority for each trunk	3-203
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	3-205
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	3-207
Queue Scheduling	Configures Weighted Round Robin queueing	3-208
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	3-210
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	3-210
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	3-212
IP Port Priority Status	Globally enables or disables IP Port Priority	3-214
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	3-214

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
QoS		3-216
DiffServ	Configure QoS classification criteria and service policies	3-216
Class Map	Creates a class map for a type of traffic	3-218
Policy Map	Creates a policy map for multiple interfaces	3-221
Service Policy	Applies a policy map defined to an ingress port	3-225
IGMP Snooping		3-226
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	3-228
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	3-230
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	3-231
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	3-232
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	3-233
DNS		3-235
General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup	3-235
Static Host Table	Configures static entries for domain name to address mapping	3-238
Cache	Displays cache entries discovered by designated name servers	3-240

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
DHCP		3-242
Relay Configuration	Specifies DHCP relay servers; enables or disables relay service	3-242
Server	Configures DHCP server parameters	3-242
General	Enables DHCP server; configures excluded address range	3-245
Pool Configuration	Configures address pools for network groups or a specific host	3-246
IP Binding	Displays addresses currently bound to DHCP clients	3-252
IP		3-265
General		3-269
Global Settings	Enables or disables routing, specifies the default gateway	3-269
Routing Interface	Configures the IP interface for the specified VLAN	3-271
ARP		3-273
General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	3-274
Static Addresses	Statically maps a physical address to an IP address	3-276
Dynamic Addresses	Shows dynamically learned entries in the IP routing table	3-277
Other Addresses	Shows internal addresses used by the switch	3-279
Statistics	Shows statistics on ARP requests sent and received	3-280

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Statistics		3-282
IP	Shows statistics for IP traffic, including the amount of traffic, address errors, routing, fragmentation and reassembly	3-282
ICMP	Shows statistics for ICMP traffic, including the amount of traffic, protocol errors, and the number of echoes, timestamps, and address masks	3-284
UDP	Shows statistics for UDP, including the amount of traffic and errors	3-287
TCP	Shows statistics for TCP, including the amount of traffic and TCP connection activity	3-288
Routing		3-266
Static Routes	Configures and display static routing entries	3-289
Routing Table	Shows all routing entries, including local, static and dynamic routes	3-290
VRRP		3-256
Group Configuration	Configures VRRP groups, including virtual interface address, advertisement interval, preemption, priority, and authentication	3-256
Global Statistics	Displays global statistics for VRRP protocol packet errors	3-262
Group Statistics	Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface	3-263

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Routing Protocol		3-268
RIP		3-292
General Settings	Enables or disables RIP, sets the global RIP version and timer values	3-293
Network Addresses	Configures the network interfaces that will use RIP	3-295
Interface Settings	Configures RIP parameters for each interface, including send and receive versions, message loopback prevention, and authentication	3-296
Statistics	Displays general information on update time, route changes and number of queries, as well as a list of statistics for known interfaces and neighbors	3-300
OSPF		3-303
General Configuration	Enables or disables OSPF; also configures the Router ID and various other global settings	3-305
Area Configuration	Specifies rules for importing routes into each area	3-309
Area Range Configuration	Configures route summaries to advertise at an area boundary	3-313
Interface Configuration	Shows area ID and designated router; also configures OSPF protocol settings and authentication for each interface	3-315
Virtual Link Configuration	Configures a virtual link through a transit area to the backbone	3-321
Network Area Address Configuration	Defines OSPF areas and associated interfaces	3-323
Summary Address Configuration	Aggregates routes learned from other protocols for advertising into other autonomous systems	3-325
Redistribute Configuration	Redistributes routes from one routing domain to another	3-327

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
NSSA Settings	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	3-329
Link State Database Information	Shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database	3-330
Border Router Information	Displays routing table entries for area border routers and autonomous system boundary routers	3-333
Neighbor Information	Displays information about neighboring routers on each interface within an OSPF area	3-334

Basic Configuration

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **MAC Address** – The physical layer address for this switch.
- **Web server** – Shows if management access via HTTP is enabled.
- **Web server port** – Shows the TCP port number used by the web interface.

- **Web secure server** – Shows if management access via HTTPS is enabled.
- **Web secure server port** – Shows the TCP port used by the HTTPS interface.
- **Telnet server** – Shows if management access via Telnet is enabled.
- **Telnet server port** – Shows the TCP port used by the Telnet interface.
- **Authentication login** – Shows the user login authentication sequence.
- **Jumbo Frame** – Shows if jumbo frames are enabled.
- **POST result** – Shows results of the power-on self-test

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)

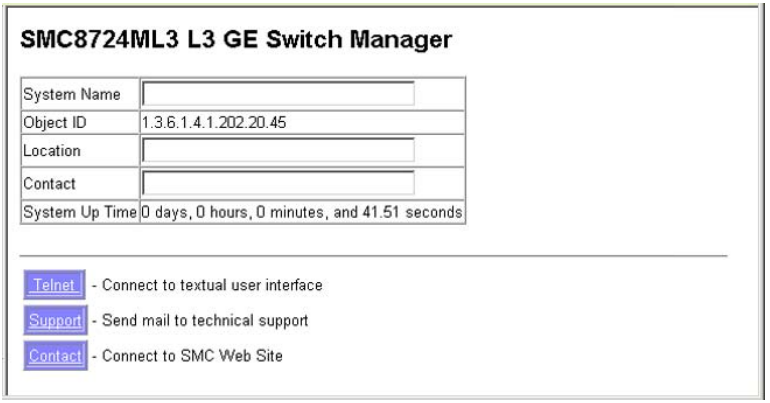


Figure 3-3 System Information

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname R&D 5                                    4-34
Console(config)#snmp-server location WC 9                         4-143
Console(config)#snmp-server contact Ted                           4-142
Console(config)#exit
Console#show system                                               4-80
System description: SMC8724ML3 L3 GE Switch
System OID string: 1.3.6.1.4.1.202.20.45
System information
 System Up time:          0 days, 1 hours, 28 minutes, and 0.51
   seconds
 System Name:             R&D 5
 System Location:         WC 9
 System Contact:          Ted
 MAC address (unit1):     00-30-F1-D4-73-A0
 Web server:              enabled
 Web server port:         80
 Web secure server:       enabled
 Web secure server port:  443
 Telnet server:           enable
 Telnet server port:      23
 Authentication login:    local RADIUS none
 Jumbo Frame:             Disabled
 POST result
UART Loopback Test ..... PASS
DRAM Test ..... PASS
Timer Test ..... PASS
PCI Device 1 Test ..... PASS
I2C Bus Initialization ..... PASS
Switch Int Loopback Test ..... PASS
Crossbar Int Loopback Test ... PASS
Fan Speed Test ..... PASS
Done All Pass.
Console#
```

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.

- **Internal Power Status** – Displays the status of the internal power supply.

Management Software

- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master or Slave.

These additional parameters are displayed for the CLI.

- **Unit ID** – Unit number in stack.
- **Redundant Power Status** – Displays the status of the redundant power supply.

Web – Click System, Switch Information.

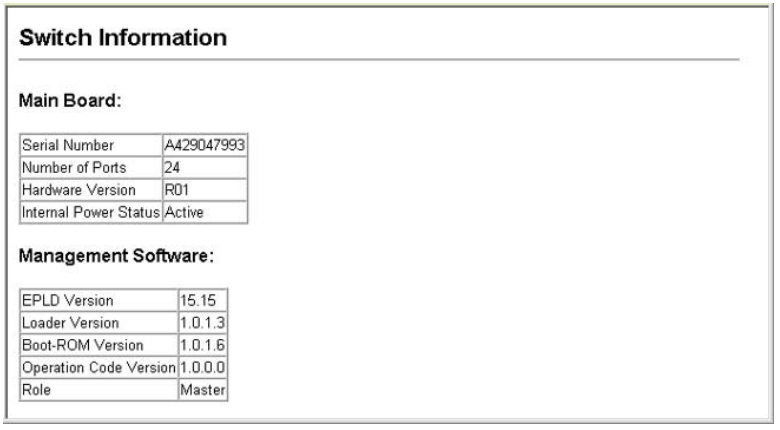


Figure 3-4 Switch Information

CLI – Use the following command to display version information.

```
Console#show version                                          4-81
Unit 1
 Serial number:            A422000632
 Hardware version:         R01
 EPLD version:             15.15
 Number of ports:          24
 Main power status:        up
 Redundant power status:   not present

Agent (master)
 Unit ID:                  1
 Loader version:           1.0.1.3
 Boot ROM version:         1.0.1.6
 Operation code version:   1.0.0.0

Console#
```

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service Configuration" on page 3-203.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 3-151.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 3-181.)

- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.

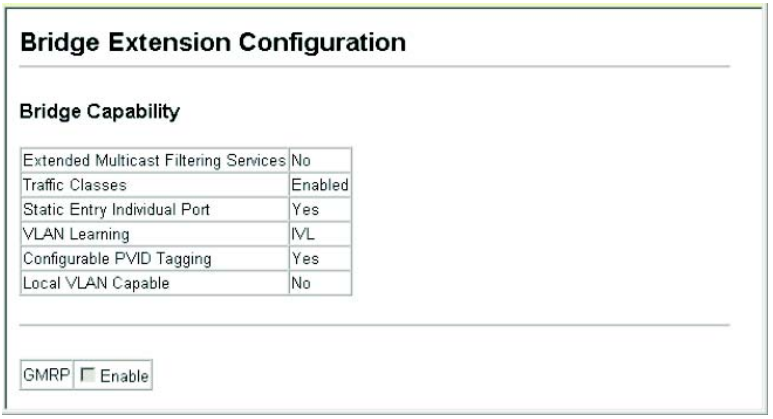


Figure 3-5 Displaying Bridge Extension Configuration

CLI – Enter the following command.

```
Console#show bridge-ext                                    4-265
 Max support VLAN numbers:              256
 Max support VLAN ID:                   4093
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Disabled
 GMRP:                                  Disabled
Console#
```

Configuring Support for Jumbo Frames

The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9000 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

Command Usage

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Command Attributes

Jumbo Packet Status – Configures support for jumbo frames. (Default: Disabled)

Web – Click System, Jumbo Frames. Enable or disable support for jumbo frames, and click Apply.



Figure 3-6 Configuring Support for Jumbo Frames

CLI – This example enables jumbo frames globally for the switch.

```
Console(config)#jumbo frame                                    4-82
Console(config)#
```

Setting the Switch's IP Address

This section describes how to configure an initial IP interface for management access over the network. The IP address for this stack is obtained via DHCP by default. To manually configure an address, you need to change the stack's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the stack and management stations that exist on another network segment (if routing is not enabled on this stack).

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Usage

- This section describes how to configure a single local interface for initial access to the stack. To configure multiple IP interfaces on this stack, you must set up an IP interface for each VLAN (page 3-271).
- To enable routing between the different interfaces on this stack, you must enable IP routing (page 3-269).
- To enable routing between the interfaces defined on this stack and external network interfaces, you must configure static routes (page page 3-289) or use dynamic routing; i.e., either RIP (page 3-292) or OSPF (page 3-303).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 3-271), static routes (page 3-289), and then dynamic routing.

Command Attributes

- **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the stack are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN to which the management station is attached. (Note you can manage the stack through any configured IP interface.) Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Default Gateway** – IP address of the gateway router between the stack and management stations that exist on other network segments. (Default: 0.0.0.0)

Manual Configuration

Web – Click IP, General, Routing Interface. Select the VLAN through which the management station is attached, set the IP Address Mode to "Static," and specify a "Primary" interface. Enter the IP address, subnet mask and gateway, then click Apply.

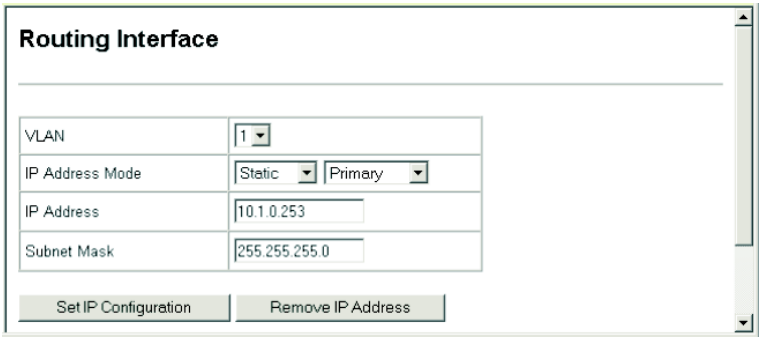


Figure 3-7 IP Interface Configuration - Manual

Click IP, Global Setting. If this stack and management stations exist on other network segments, then specify the default gateway, and click Apply.

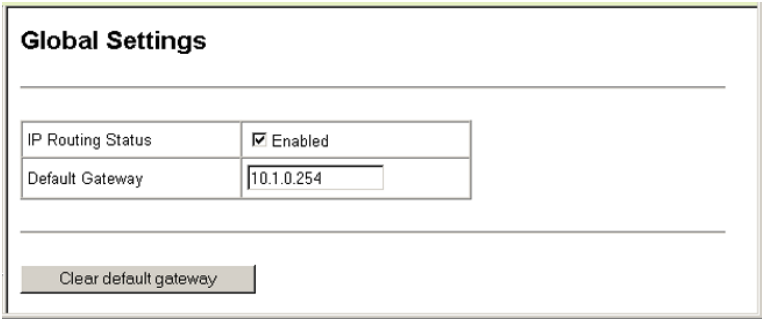


Figure 3-8 Default Gateway

CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1                                    4-187
Console(config-if)#ip address 10.1.0.253 255.255.255.0              4-308
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                       4-310
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the stack to be dynamically configured by these services.

Web – Click IP, General, Routing Interface. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the stack will also broadcast a request for IP configuration settings on each power reset.

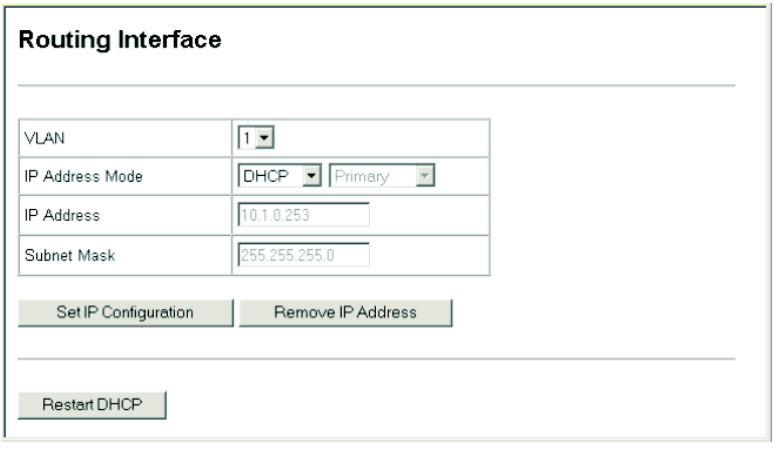


Figure 3-9 IP Interface Configuration - DHCP

Note: If you lose your management connection, make a console connection to the Master unit and enter "show ip interface" to determine the new stack address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the "ip dhcp restart client" command.

```
Console#config
Console(config)#interface vlan 1                                    4-187
Console(config-if)#ip address dhcp                                  4-308
Console(config-if)#end
Console#ip dhcp restart client                                      4-158
Console#show ip interface                                           4-311

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.1.253, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the stack is moved to another network segment, you will lose management access to the stack. In this case, you can reboot the stack or submit a client request to restart DHCP service via the CLI.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart client                                      4-158
Console#
```

Managing Firmware

You can upload/download firmware to or from a TFTP server, or copy files to and from switch units in a stack. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version. You must specify the method of file transfer, along with the file type and file names as required.

Command Attributes

- File Transfer Method – The firmware copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
  - file to unit – Copies a file from this switch to another unit in the stack.
  - unit to file – Copies a file from another unit in the stack to this switch.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify opcode (operational code) to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- **Source/Destination Unit** – Stack unit. (Range: 1 - 8)

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloading System Software from a Server

When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, File Management, Copy Operation. Select "tftp to file" as the file transfer method, enter the IP address of the TFTP server, set the file type to "opcode," enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Apply. If you replaced the current firmware used for startup and want to start using the new operation code, reboot the system via the System/Reset menu.

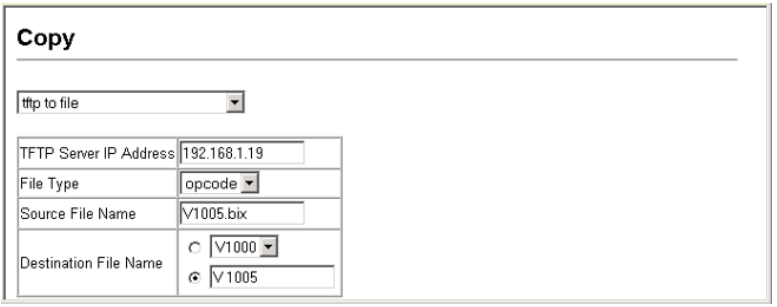


Figure 3-10 Copy Firmware

If you download to a new destination file, go to the File Management, Set Start-Up menu, mark the operation code file used at startup, and click Apply. To start the new firmware, reboot the system via the System/Reset menu.

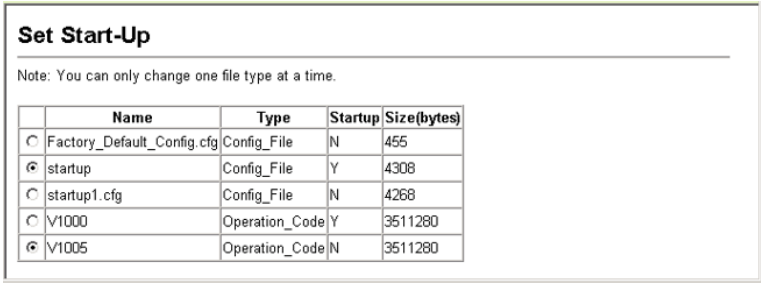


Figure 3-11 Setting the Startup Code

To delete a file select System, File Management, Delete. Select the file name from the given list by checking the tick box and click Apply. Note that the file currently designated as the startup code cannot be deleted.

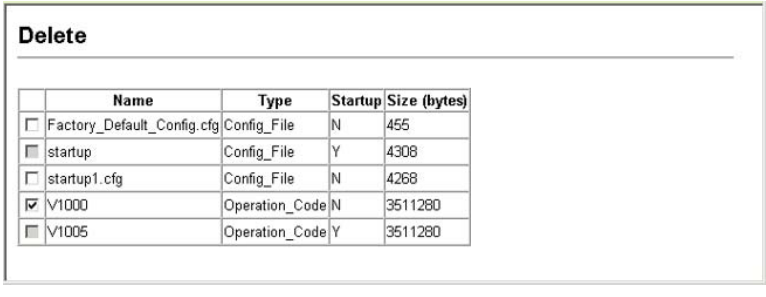


Figure 3-12 Deleting Files

CLI – To download new firmware form a TFTP server, enter the IP address of the TFTP server, select "config" as the file type, then enter the source and destination file names. When the file has finished downloading, set the new file to start up the system, and then restart the switch.

To start the new firmware, enter the "reload" command or reboot the system.

```
Console#copy tftp file                                          4-84
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: V1005.bix
Destination file name: V1005
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V1005                        4-90
Console(config)#exit
Console#reload                                                  4-30
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server, or copy files to and from switch units in a stack. The configuration file can be later downloaded to restore the switch's settings.

Command Attributes

- File Transfer Method – The configuration copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to running-config – Copies a file in the switch to the running configuration.
  - file to startup-config – Copies a file in the switch to the startup configuration.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - running-config to file – Copies the running configuration to a file.
  - running-config to startup-config – Copies the running config to the startup config.

- running-config to tftp – Copies the running configuration to a TFTP server.
- startup-config to file – Copies the startup configuration to a file on the switch.
- startup-config to running-config – Copies the startup config to the running config.
- startup-config to tftp – Copies the startup configuration to a TFTP server.
- tftp to file – Copies a file from a TFTP server to the switch.
- tftp to running-config – Copies a file from a TFTP server to the running config.
- tftp to startup-config – Copies a file from a TFTP server to the startup config.
- file to unit – Copies a file from this switch to another unit in the stack.
- unit to file – Copies a file from another unit in the stack to this switch.

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify config (configuration) to copy configuration settings.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- **Source/Destination Unit** – Stack unit. (Range: 1 - 8)

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, File Management, Copy Operation. Choose "tftp to startup-config" or "tftp to file," and enter the IP address of the TFTP server. Specify the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Apply.

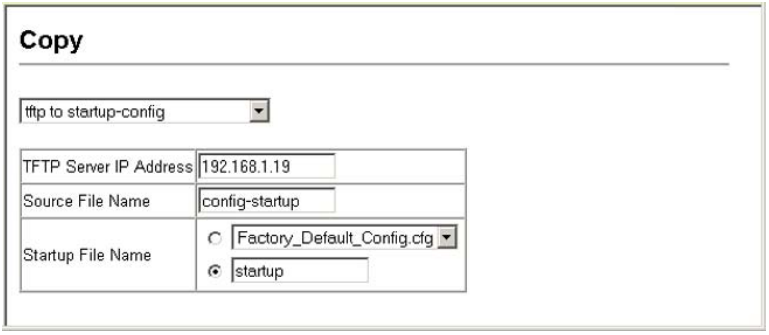


Figure 3-13 Downloading Configuration Settings for Start-Up

If you download to a new file name using "tftp to startup-config" or "tftp to file," the file is automatically set as the start-up configuration file. To use the new settings, reboot the system via the System/Reset menu. You can also select any configuration file as the start-up configuration by using the System/File Management/Set Start-Up page.

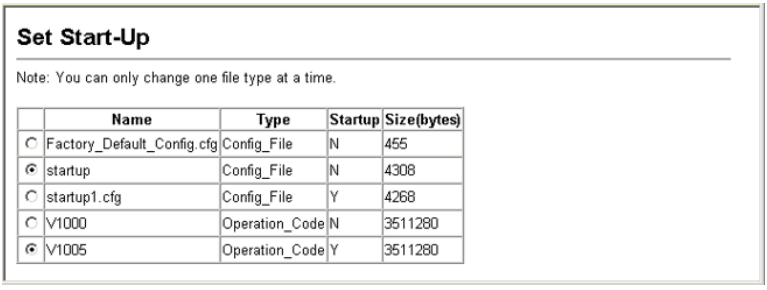


Figure 3-14 Setting the Startup Configuration Settings

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                    4-84
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

To select another configuration file as the start-up configuration, use the **boot system** command and then restart the switch.

```
Console#config
Console(config)#boot system config: startup                         4-90
Console(config)#exit
Console#reload                                                      4-30
```

Console Port Settings

You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial console port. Management access through the console port is controlled by various parameters, including a password, timeouts, and basic communication settings. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 0)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 0 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535; Default: 0)
- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)
- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the

device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud, Auto; Default: Auto)

- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)
- **Password**[2] – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login** – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Console. Specify the console port connection parameters as required, then click Apply.

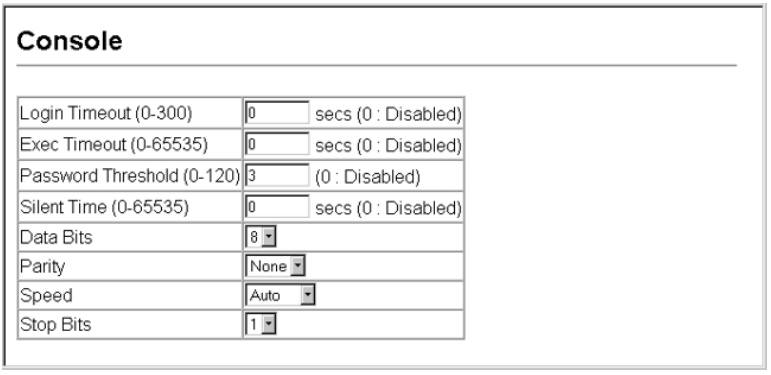

Console
Login Timeout (0-300) 0 secs (0 : Disabled)
Exec Timeout (0-65535) 0 secs (0 : Disabled)
Password Threshold (0-120) 3 (0 : Disabled)
Silent Time (0-65535) 0 secs (0 : Disabled)
Data Bits 8
Parity None
Speed Auto
Stop Bits 1

Figure 3-15 Configuring the Console Port

2. CLI only.

CLI – Enter Line Configuration mode for the console, then specify the connection parameters as required. To display the current console port settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line console                                    4-15
Console(config-line)#login local                                4-16
Console(config-line)#password 0 secret                          4-17
Console(config-line)#timeout login response 0                   4-18
Console(config-line)#exec-timeout 0                             4-19
Console(config-line)#password-thresh 5                          4-20
Console(config-line)#silent-time 60                             4-21
Console(config-line)#databits 8                                 4-21
Console(config-line)#parity none                                4-22
Console(config-line)#speed auto                                 4-23
Console(config-line)#stopbits 1                                 4-24
Console(config-line)#end
Console#show line console                                       4-25
 Console configuration:
  Password threshold:  5 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         60
  Baudrate:            auto
  Databits:            8
  Parity:              none
  Stopbits:            1
Console#
```

Telnet Settings

You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other various parameters set, including the TCP port number, timeouts, and a password. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **Telnet Port Number** – Sets the TCP port number for Telnet on the switch. (Default: 23)
- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout

interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 300 seconds)

- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Password**[3] – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login** – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Telnet. Specify the connection parameters for Telnet access, then click Apply.

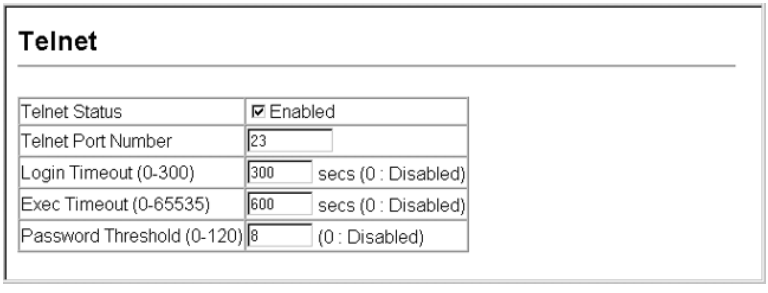


Figure 3-16 Configuring the Telnet Interface

3. CLI only.

CLI – Enter Line Configuration mode for a virtual terminal, then specify the connection parameters as required. To display the current virtual terminal settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line vty                                    4-15
Console(config-line)#login local                            4-16
Console(config-line)#password 0 secret                      4-17
Console(config-line)#timeout login response 300             4-18
Console(config-line)#exec-timeout 600                       4-19
Console(config-line)#password-thresh 3                      4-20
Console(config-line)#end
Console#show line vty                                       4-25
 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:       300 sec
Console#
```

Configuring Event Logging

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

System Log Configuration

The system allows you to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 3-3 Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, Logs, System Logs. Specify System Log Status, set the level of event messages to be logged to RAM and flash memory, then click Apply.

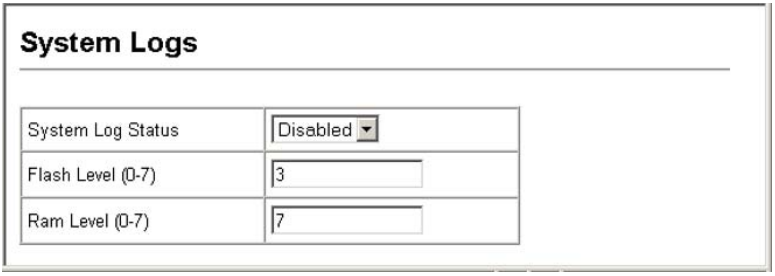


Figure 3-17 System Logs

CLI – Enable system logging and then specify the level of messages to be logged to RAM and flash memory. Use the **show logging** command to display the current settings.

```
Console(config)#logging on                                    4-58
Console(config)#logging history ram 0                         4-58
Console(config)#
Console#show logging ram                                      4-62
Syslog logging:           Disabled
History logging in RAM: level emergencies
Console#
```

Remote Log Configuration

The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages at or above a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

  The attribute specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Host IP List** – Displays the list of remote server IP addresses that will receive syslog messages. The maximum number of host IP addresses allowed is five.
- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

Web – Click System, Logs, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add. To delete an IP address, click the entry in the Host IP List, and then click Remove.

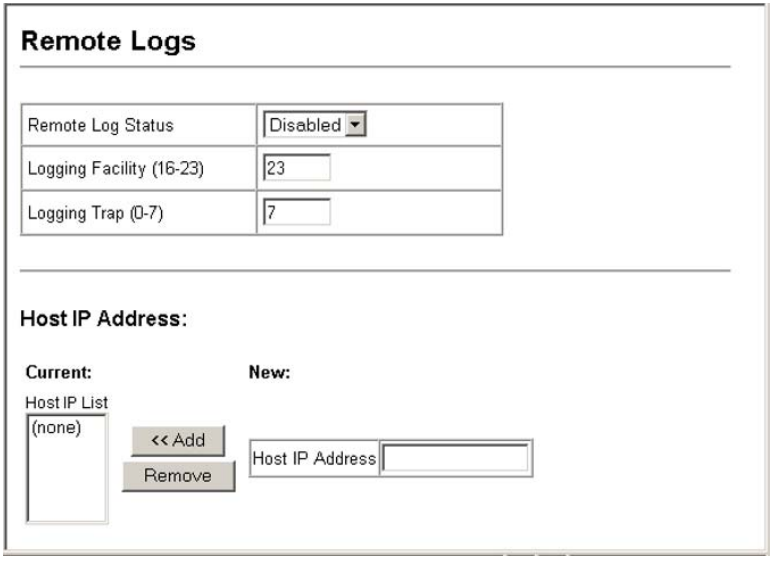


Figure 3-18 Remote Logs

CLI – Enter the syslog server host IP address, choose the facility type and set the logging trap.

```
Console(config)#logging host 10.1.0.9                              4-60
Console(config)#logging facility 23                                4-60
Console(config)#logging trap 4                                     4-61
Console(config)#logging trap
Console(config)#exit
Console#show logging trap                                          4-62
Syslog logging:               Enabled
REMOTELOG status:             Disabled
REMOTELOG facility type:      local use 7
REMOTELOG level type:         Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Displaying Log Messages

Use the Logs page to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Log, Logs.

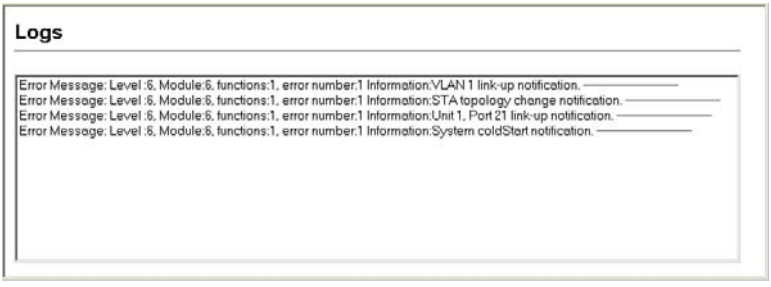

Logs
Error Message: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:STA topology change notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 21 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification.

Figure 3-19 Displaying Logs

CLI – This example shows the event message stored in RAM.

```
Console#show log ram                                          4-64
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

Sending Simple Mail Transfer Protocol Alerts

To alert system administrators of problems, the switch can use SMTP (Simple Mail Transfer Protocol) to send email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

Command Attributes

- **Admin Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Email Source Address** – Sets the email address used for the "From" field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.
- **Severity** – Sets the syslog severity threshold level (see table on page 3-39) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- **SMTP Server List** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails. Use the New SMTP Server text field and the Add/Remove buttons to configure the list.
- **Email Destination Address List** – Specifies the email recipients of alert messages. You can specify up to five recipients. Use the New Email Destination Address text field and the Add/Remove buttons to configure the list.

Web – Click System, Log, SMTP. Enable SMTP, specify a source email address, and select the minimum severity level. To add an IP address to the SMTP Server List, type the new IP address in the SMTP Server field and click Add. To delete an IP address, click the entry in the SMTP Server List and click Remove. Specify up to five email addresses to receive the alert messages, and click Apply.

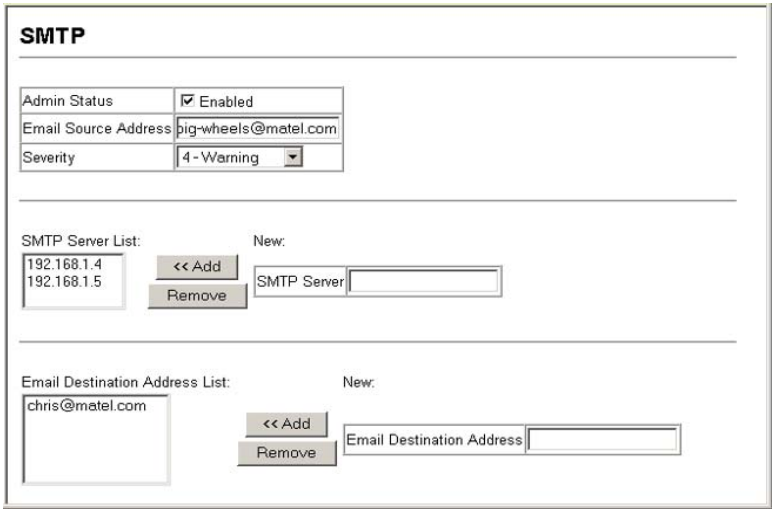


Figure 3-20 Enabling and Configuring SMTP Alerts

CLI – Enter the IP address of at least one SMTP server, set the syslog severity level to trigger an email message, and specify the switch (source) and up to five recipient (destination) email addresses. Enable SMTP with the **logging sendmail** command to complete the configuration. Use the **show logging sendmail** command to display the current SMTP configuration.

```
Console(config)#logging sendmail host 192.168.1.4              4-65
Console(config)#logging sendmail level 3                       4-66
Console(config)#logging sendmail source-email
   big-wheels@matel.com                                        4-67
Console(config)#logging sendmail destination-email
   chris@matel.com                                             4-68
Console(config)#logging sendmail                               4-68
Console(config)#exit
Console#show logging sendmail                                  4-69
SMTP servers
-------------------------------------------
  1. 192.168.1.4

SMTP minimum severity level: 4

SMTP destination email addresses
-------------------------------------------
  1. chris@matel.com

SMTP source email address: big-wheels@matel.com

SMTP status:                Enabled
Console#
```

Renumbering the Stack

If the units are no longer numbered sequentially after several topology changes or failures, you can reset the unit numbers using the "Renumbering" command. Just remember to save the new configuration settings to a startup configuration file prior to powering off the stack Master.

Command Usage

- The startup configuration file maps configuration settings to each switch in the stack based on the unit identification number. You should therefore remember to save the current configuration after renumbering the stack.
- For a line topology, the stack is numbered from top to bottom, with the first unit in the stack designated at unit 1. For a ring topology, the Master unit taken as the top of the stack and is numbered as unit 1, and all other units are numbered sequentially down through the ring.

Web – Click System, Renumbering.



Figure 3-21 Renumbering the Stack

CLI – This example renumbers all units in the stack.

```
Console#switch all renumber                                    4-34
Console#
```

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch. When prompted, confirm that you want reset the switch.



Figure 3-22 Resetting the System

CLI – Use the reload command to restart the switch.

```
Console#reload                                                 4-30
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See "calendar set" on page 4-74.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Configuring SNTP

You can configure the switch to send time synchronization requests to time servers.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP client. This requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)
- **SNTP Server** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.

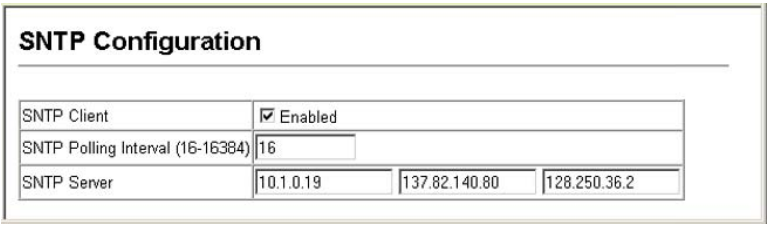


Figure 3-23 SNTP Configuration

CLI – This example configures the switch to operate as an SNTP client and then displays the current time and settings.

```
Console(config)#sntp client                                    4-70
Console(config)#sntp poll 16                                   4-72
Console(config)#sntp server 10.1.0.19 137.82.140.80
  128.250.36.2                                                 4-71
Console(config)#exit
Console#show sntp                                              4-73
Current time:  Jan  6 14:56:05 2004
Poll interval: 60
Current  mode:  unicast
SNTP status : Enabled
SNTP server 10.1.0.19 137.82.140.80 128.250.36.2
Current server: 128.250.36.2
Console#
```

Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours (0-13)** – The number of hours before/after UTC.

- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.

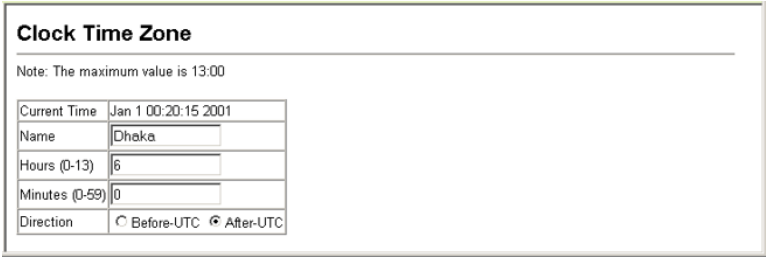


Figure 3-24 Clock Time Zone

CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC4-73
Console#
```

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the

MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as SMC EliteView. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch using from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The switch has a default view (all MIB objects) and default groups defined for security models v1

and v2c. The following table shows the security models and levels available and the system default settings.

Table 3-4 SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuth NoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuth NoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuth NoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuth NoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	A user name match only
v3	Auth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

Note: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

Enabling the SNMP Agent

Enables SNMPv3 service for all management clients (i.e., versions 1, 2c, 3).

Command Attributes

SNMP Agent Status – Enables SNMP on the switch.

Web – Click SNMP, Agent Status. Enable the SNMP Agent by marking the Enabled checkbox, and click Apply.



Figure 3-25 Enabling the SNMP Agent

CLI – The following example enables SNMP on the switch.

```
Console(config)#snmp-server                                    4-140
Console(config)#
```

Setting Community Access Strings

You may configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – The switch supports up to five community strings.
- **Current** – Displays a list of the community strings currently configured.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

  Default strings: "public" (read-only access), "private" (read/write access)
  Range: 1-32 characters, case sensitive

- **Access Mode** – Specifies the access rights for the community string:
  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.



Figure 3-26 Configuring SNMP Community Strings

CLI – The following example adds the string "spiderman" with read/write access.

```
Console(config)#snmp-server community spiderman rw              4-141
Console(config)#
```

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as SMC EliteView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- If you specify an SNMP Version 3 host, then the "Trap Manager Community String" is interpreted as an SNMP user name. If you use V3 authentication or encryption options (authNoPriv or authPriv), the user name must first be defined in the SNMPv3 Users page (page 3-60). Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the no authentication (noAuth) option, an SNMP user account will be automatically generated, and the switch will authorize SNMP access for the host.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 3-53).
  2. Enable trap informs as described in the following pages.
  3. Create a view with the required notification messages (page 3-72).
  4. Create a group that includes the required notify view (page 3-66).

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 3-53).
  2. Enable trap informs as described in the following pages.
  3. Create a view with the required notification messages (page 3-72).
  4. Create a group that includes the required notify view (page 3-66).
  5. Specify a remote engine ID where the user resides (page 3-59).
  6. Then configure a remote user (page 3-63).

Command Attributes

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Current** – Displays a list of the trap managers currently configured.
- **Trap Manager IP Address** – IP address of a new management station to receive notification messages.
- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. Though you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Configuration page (for Version 1 or 2c clients), or define a corresponding "User Name" in the SNMPv3 Users page (for Version 3 clients). (Range: 1-32 characters, case sensitive)
- **Trap UDP Port** – Specifies the UDP port number used by the trap manager.
- **Trap Version** – Indicates if the user is running SNMP v1, v2c, or v3. (Default: v1)
- **Trap Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Trap Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
  - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

- **Enable Authentication Traps**[4] – Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)
- **Enable Link-up and Link-down Traps** – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

Web – Click SNMP, Configuration. Enter the IP address and community string for each management station that will receive trap messages, specify the port, trap version, trap security level (for v3 clients), trap inform settings (for v2c/v3 clients), and then click Add. Select the trap types required using the check boxes for Authentication and Link-up/down traps, and then click Apply.

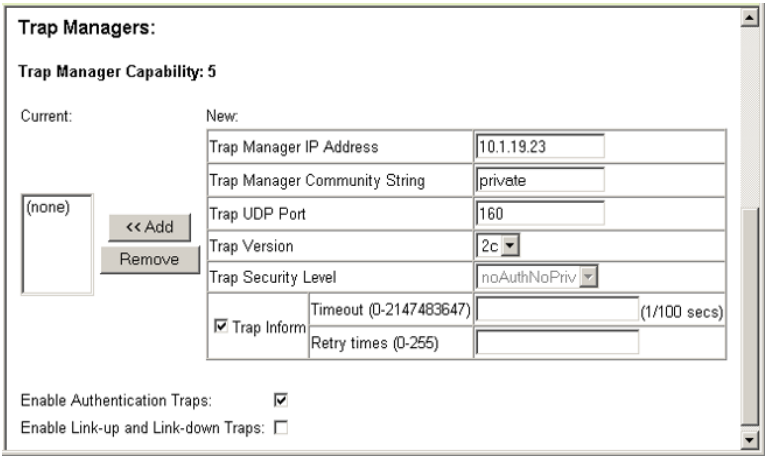


Figure 3-27 Configuring SNMP Trap Managers

CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 private version 2c
 udp-port 162                                                    4-143
Console(config)#snmp-server enable traps authentication          4-146
```

4. These are legacy notifications and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 3-66).

Configuring SNMPv3 Management Access

To configure SNMPv3 management access to the switch, follow these steps:

1. If you want to change the default engine ID, do so before configuring other SNMP parameters.
2. Specify read and write access views for the switch MIB tree.
3. Configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).
4. Assign SNMP users to groups, along with their specific authentication and privacy passwords.

Setting an Engine ID

An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

A new engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

Web – Click SNMP, SNMPv3, Engine ID. Enter an ID of up to 26 hexadecimal characters and then click Save.

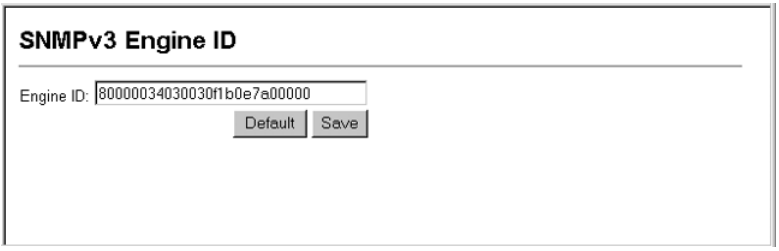


Figure 3-28 Setting the SNMPv3 Engine ID

CLI – This example sets an SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id local 12345abcdef       4-147
Console(config)#exit
Console#show snmp engine-id                                   4-149
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1
Console#
```

Specifying a Remote Engine ID

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Specifying Trap Managers and Trap Types" on page 3-54 and "Configuring Remote SNMPv3 Users" on page 3-63.)

The engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value "1234" is equivalent to "1234" followed by 22 zeroes.

Web – Click SNMP, SNMPv3, Remote Engine ID. Enter an ID of up to 26 hexadecimal characters and then click Save.

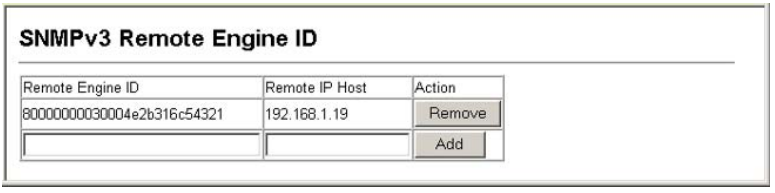


Figure 3-29 Setting an Engine ID

CLI – This example specifies a remote SNMPv3 engine ID.

```
Console(config)#snmp-server engineID remote 54321 192.168.1.19      4-147
Console(config)#exit
Console#show snmp engine-id                                         4-149
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                          IP address
80000000030004e2b316c54321                                    192.168.1.19
Console#
```

Configuring SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read and a write view.

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.

- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.
- **Actions** – Enables the user to be assigned to another SNMPv3 group.

Web – Click SNMP, SNMPv3, Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.

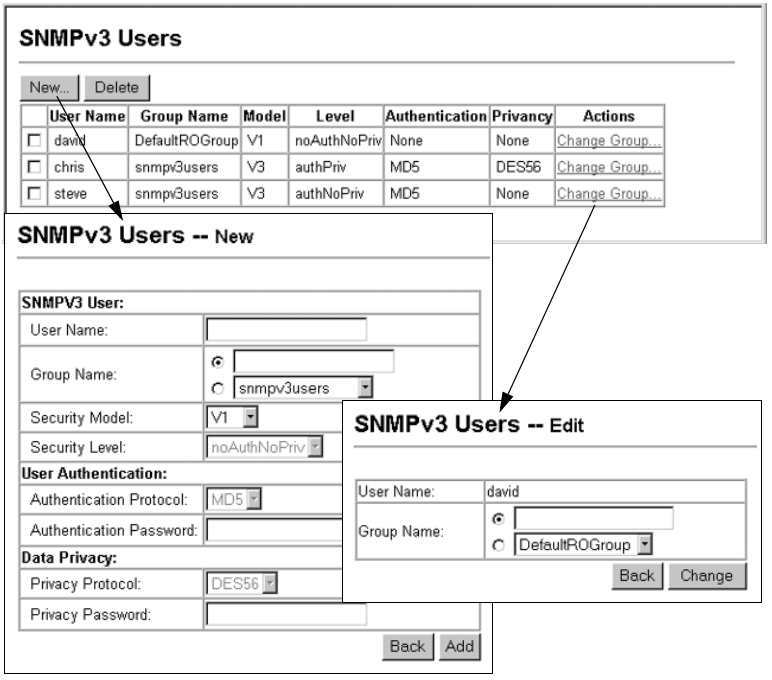


Figure 3-30 Configuring SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user chris group r&d v3 auth md5
 greenpeace priv des56 einstien                                    4-154
Console(config)#exit
Console#show snmp user                                             4-156
EngineId: 80000034030001f488f5200000
User Name: chris
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring Remote SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read and a write view.

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. (See "Specifying Trap Managers and Trap Types" on page 3-54 and "Specifying a Remote Engine ID" on page 3-59.)

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Engine ID** – The engine identifier for the SNMP agent on the remote device where the remote user resides. Note that the remote engine identifier must be specified before you configure a remote user. (See "Specifying a Remote Engine ID" on page 3-59.)
- **Remote IP** – The Internet address of the remote device where the user resides.
- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v1)
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

Web – Click SNMP, SNMPv3, Remote Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete.

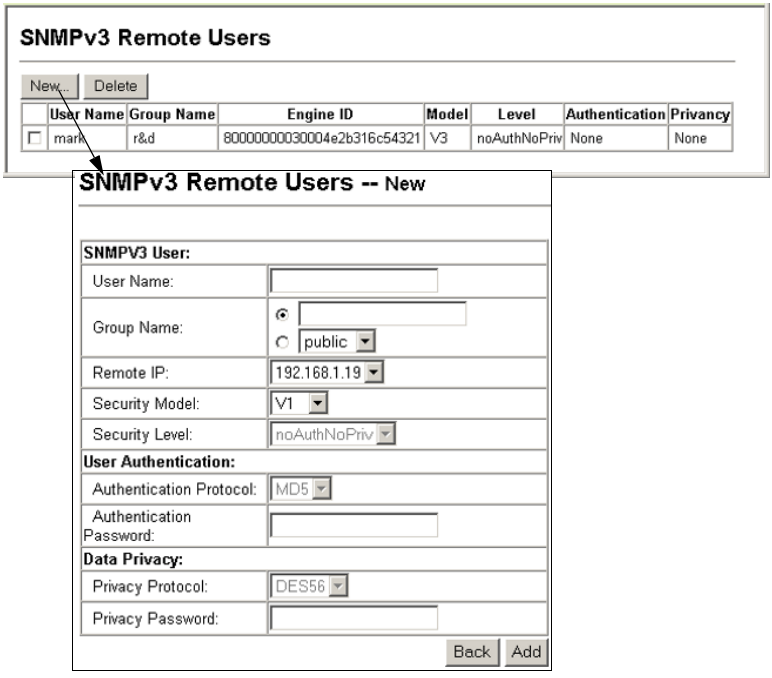


Figure 3-31 Configuring Remote SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user mark group r&d remote
 192.168.1.19 v3 auth md5 greenpeace priv des56 einstien      4-154
Console(config)#exit
Console#show snmp user                                        4-156
No user exist.

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring SNMPv3 Groups

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

Command Attributes

- **Group Name** – The name of the SNMP group. (Range: 1-32 characters)
- **Model** – The group security model; SNMP v1, v2c or v3.
- **Level** – The security level used for the group:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications.
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Read View** – The configured view for read access. (Range: 1-64 characters)
- **Write View** – The configured view for write access. (Range: 1-64 characters)

- **Notify View** – The configured view for notifications. (Range: 1-64 characters)

Table 3-5 Supported Notification Messages

Object Label	Object ID	Description
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.

Table 3-5 Supported Notification Messages (Continued)

Object Label	Object ID	Description
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

Table 3-5 Supported Notification Messages (Continued)

Object Label	Object ID	Description
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.
Private Traps		
swPowerStatus ChangeTrap	1.3.6.1.4.1.202.6.10.65.2.1.0.1	This trap is sent when the power state changes.
swFanFailureTrap	1.3.6.1.4.1.202.6.10.65.2.1.0.17	This trap is sent when the fan fails.
swFanRecoverTrap	1.3.6.1.4.1.202.6.10.65.2.1.0.18	This trap is sent when the fan failure has recovered.
swIpFilterRejectTrap	1.3.6.1.4.1.202.6.10.65.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swSmtpConnFailure Trap	1.3.6.1.4.1.202.6.10.65.2.1.0.41	This trap is triggered if the SMTP system cannot open a connection to the mail server successfully.
swMainBoardVer MismatchNotificaiton	1.3.6.1.4.1.202.6.10.65.2.1.0.56	This trap is sent when the slave board version is mismatched with the master board version. This trap binds two objects, the first object indicates the master version, whereas the second represents the slave version.
swModuleVer MismatchNotificaiton	1.3.6.1.4.1.202.6.10.65.2.1.0.57	This trap is sent when the slide-in module version is mismatched with the main board version.

Table 3-5 Supported Notification Messages (Continued)

Object Label	Object ID	Description
swThermalRising Notification	1.3.6.1.4.1.202.6.10.65.2.1.0.58	This trap is sent when the temperature exceeds the switchThermalActionRisingThreshold.
swThermalFalling Notification	1.3.6.1.4.1.202.6.10.65.2.1.0.59	This trap is sent when the temperature falls below the switchThermalActionFallingThreshold.
swModuleInsertion Notificaiton	1.3.6.1.4.1.202.6.10.65.2.1.0.60	This trap is sent when a module is inserted.
swModuleRemoval Notificaiton	1.3.6.1.4.1.202.6.10.65.2.1.0.61	This trap is sent when a module is removed.

*These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu (page 3-57).

Web – Click SNMP, SNMPv3, Groups. Click New to configure a new group. In the New Group page, define a name, assign a security model and level, and then select read and write views. Click Add to save the new group and return to the Groups list. To delete a group, check the box next to the group name, then click Delete.

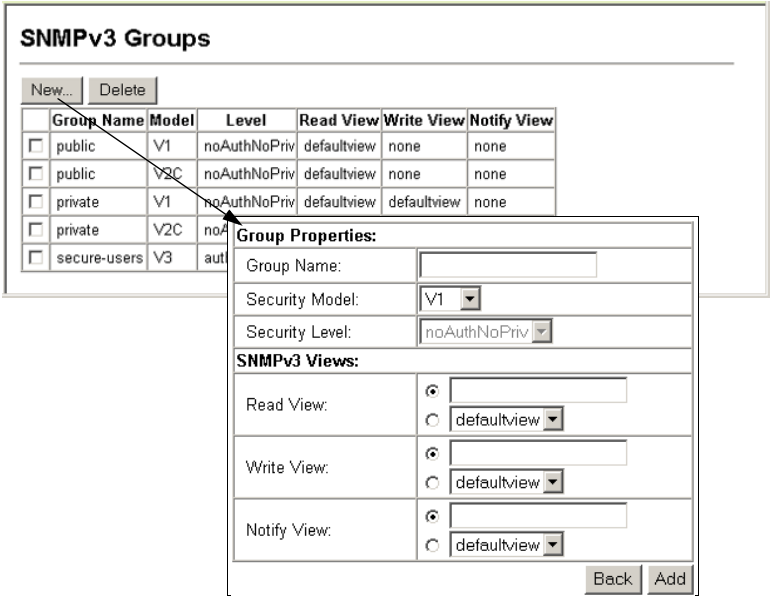


Figure 3-32 Configuring SNMPv3 Groups

CLI – Use the **snmp-server group** command to configure a new group, specifying the security model and level, and restricting MIB access to defined read and write views.

```
Console(config)#snmp-server group secure-users v3 priv read
 defaultview write defaultview notify defaultview            4-152
Console(config)#exit
Console#show snmp group                                      4-153
:
Group Name: secure-users
Security Model: v3
Read View: defaultview
Write View: defaultview
Notify View: defaultview
Storage Type: nonvolatile
Row Status: active

Console#
```

Setting SNMPv3 Views

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

Command Attributes

- **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- **View OID Subtrees** – Shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view.
- **Edit OID Subtrees** – Allows you to configure the object identifiers of branches within the MIB tree. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Web – Click SNMP, SNMPv3, Views. Click New to configure a new view. In the New View page, define a name and specify OID subtrees in the switch MIB to be included or excluded in the view. Click Back to save the new view and return to the SNMPv3 Views list. For a specific view, click on View OID Subtrees to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings. To delete a view, check the box next to the view name, then click Delete.

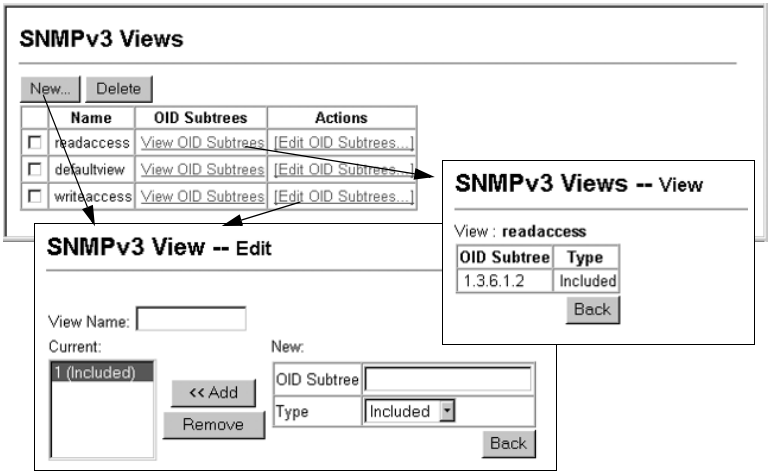


Figure 3-33 Configuring SNMPv3 Views

CLI – Use the **snmp-server view** command to configure a new view. This example view includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
  included                                                    4-150
Console(config)#exit
Console#show snmp view                                        4-151
View Name: ifEntry.a
Subtree OID: 1.3.6.1.2.1.2.2.1.1.*
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: readaccess
Subtree OID: 1.3.6.1.2
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```

User Authentication

You can restrict management access to this switch and provide secure network access using the following options:

- User Accounts – Manually configure management access rights for users.
- Authentication Settings – Use remote authentication to configure access rights.
- HTTPS Settings – Provide a secure web connection.
- SSH Settings – Provide a secure shell (for secure Telnet access).
- Port Security – Configure secure addresses for individual ports.
- 802.1X – Use IEEE 802.1X port authentication to control access to specific ports.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.

Configuring User Accounts

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

The default guest name is "guest" with the password "guest." The default administrator name is "admin" with the password "admin."

Command Attributes

- **Account List** – Displays the current list of user accounts and associated access levels. (Defaults: admin, and guest)
- **New Account** – Displays configuration settings for a new account.
  - **User Name** – The name of the user.
    (Maximum length: 8 characters; maximum number of users: 16)
  - **Access Level** – Specifies the user level.
    (Options: Normal and Privileged)
  - **Password** – Specifies the user password.
    (Range: 0-8 characters plain text, case sensitive)
- **Change Password** – Sets a new password for the specified user.

Web – Click Security, User Accounts. To configure a new user account, enter the user name, access level, and password, then click Add. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again, then click Apply.

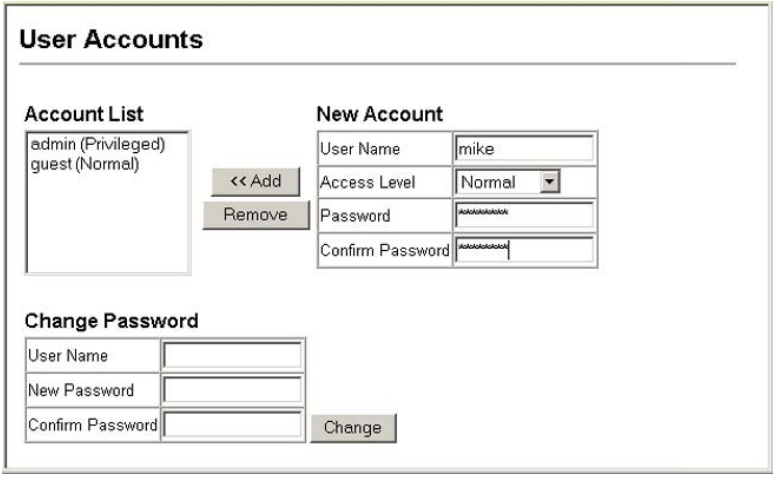


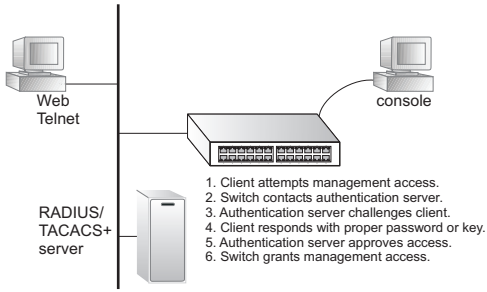
Figure 3-34 User Accounts

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                    4-35
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.



Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS- aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not

available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **Radius** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.
- **RADIUS Settings**
  - **Global** – Provides globally applicable RADIUS settings.
  - **ServerIndex** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
  - **Server IP Address** – Address of authentication server. (Default: 10.1.0.1)
  - **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
  - **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
  - **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

- **TACACS Settings**
  - **Server IP Address** – Address of the TACACS+ server. (Default: 10.11.12.13)
  - **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See "username" on page 4-35.)

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.

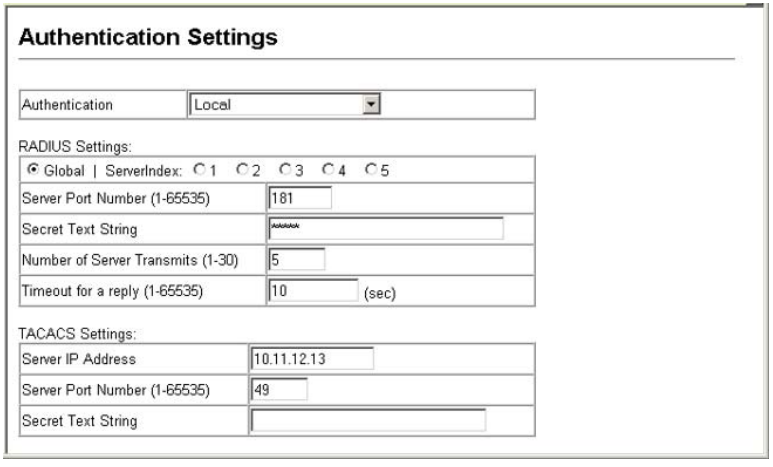


Figure 3-35 Authentication Server Settings

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                    4-92
Console(config)#radius-server port 181                         4-96
Console(config)#radius-server key green                        4-96
Console(config)#radius-server retransmit 5                     4-97
Console(config)#radius-server timeout 10                       4-97
Console(config)#radius-server 1 host 192.168.1.25              4-95
Console(config)#exit
Console#show radius-server                                     4-98

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   181
 Retransmit times:                     5
 Request timeout:                      10

Server 1:
 Server IP address: 192.168.1.25
 Communication key with RADIUS server: *****
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10


Console#config
Console(config)#authentication login tacacs                    4-92
Console(config)#tacacs-server host 10.20.30.40                 4-99
Console(config)#tacacs-server port 200                         4-100
Console(config)#tacacs-server key green                        4-100
Console(config)#exit
Console#show tacacs-server                                     4-101
Server IP address:                   10.20.30.40
 Communication key with tacacs server: *****
 Server port number:                  200
Console(config)#
```

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.

- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 6.2 or above.
- The following web browsers and operating systems currently support HTTPS:

Table 3-6 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 3-82.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. (Default: Port 443)

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.

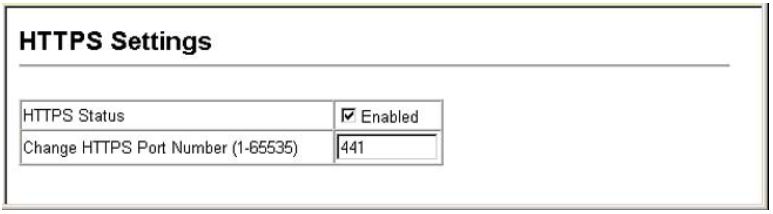


Figure 3-36 HTTPS Settings

CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server                    4-42
Console(config)#ip http secure-port 441                  4-43
Console(config)#
```

Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Note: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate                                    4-84
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type "reload" at the command prompt:

```
Console#reload
```

Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Command Usage

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the **Authentication Settings** page (page 3-76). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.
2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956 10825913212890233
   76546801726272571413428762941301196195566782 59566410486957427888146206
   51941746772984865468615717739390164779355942303577413098022737087794545240839
   71752646358058176716709574804776117

3. *Import Client's Public Key to the Switch* – Use the **copy tftp public-key** command (page 4-84) to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 3-75.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

1024 35 134108168560989392104094492015542534763164192187295892114317388
0555361616310517759408386863110929123222682851925437460310093718772119969631
7813662774141689851320491172048303392543241016379975923714490119380060902539484
0848271781943722884025331159521348610229029789827213532671316294325328189150
45306393916643 steve@192.168.1.19

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

6. *Challenge-Response Authentication* – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:
   a. The client sends its public key to the switch.
   b. The switch compares the client's public key to those stored in memory.
   c. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
   d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.
   e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Notes: **1.** To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

2. The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the preceding section (Command Usage).

Field Attributes

- **Public-Key of Host-Key** – The public key for the host.
  - RSA (Version 1): The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA (Version 2): The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both: Default: Both)

  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory to flash memory). Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.
- **Generate** – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.
- **Clear** – This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

Web – Click Security, SSH, Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click Generate.

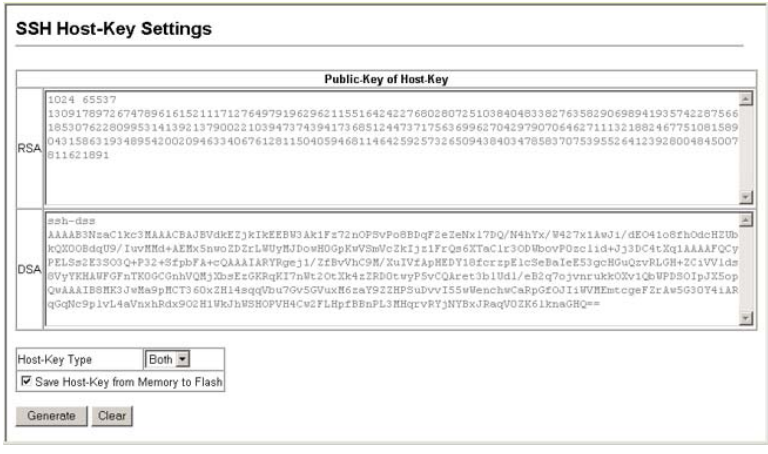


Figure 3-37 SSH Host-Key Settings

CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate                          4-48
Console#ip ssh save host-key                                     4-48
Console#show public-key host                                     4-48
Host:
RSA:
1024 65537
12725092254492640213133651454613118967905519236007602865300676l
8240969094744832010252487896597759216832222558465238779154647980739
631403386925793105105765212243052807865885485789272602937866089236 8
414232759121276032591968369705343933643844522333518828717389689451 1
729290510813919642025190932104328579045764891
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasf
EthIwmjhLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9X
Ts7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZA
AAAFQCNZn/x17dwpW8RrV DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1Tmrm
SiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5il
c3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG Nq375R55yRxFvmcGIn/Q7IphPqyJ3o
9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOIRTMFy3iUXtvGyQAOVSy67Mf
c3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAgPNWKV6W0hqmshQdo
tVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

Configuring the SSH Server

The SSH server includes basic settings for authentication.

Field Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1 to 120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

- **SSH Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default: 768)
  - The server key is a private key that is never shared outside the switch.
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.

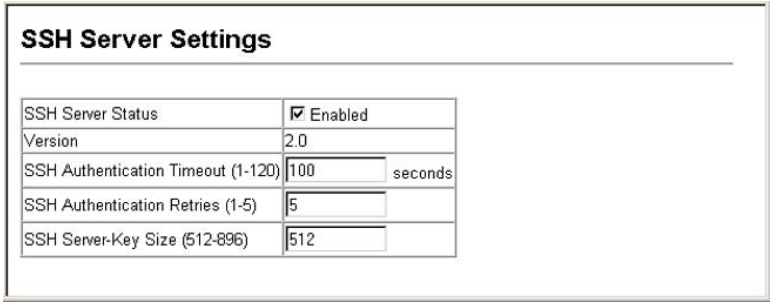


Figure 3-38 SSH Server Settings

CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disables this connection.

```
Console(config)#ip ssh server                                          4-48
Console(config)#ip ssh timeout 100                                     4-49
Console(config)#ip ssh authentication-retries 5                        4-50
Console(config)#ip ssh server-key size 512                             4-51
Console(config)#end
Console#show ip ssh                                                    4-54
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh                                                       4-55
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   2.0      cipher-3des   session-started
Console#disconnect 0                                                   4-24
Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (page 3-151). When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

Command Usage

- A secure port has the following restrictions:
  - It cannot use port monitoring.
  - It cannot be a multi-VLAN port.
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1 - 1024 for the port to allow access.

- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (page 3-122).

Command Attributes

- **Port** – Port number.
- **Name** – Descriptive text (page 4-187).
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
- **Trunk** – Trunk number if port is a member (page 3-126 and 3-128).

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, mark the checkbox in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port, and click Apply.

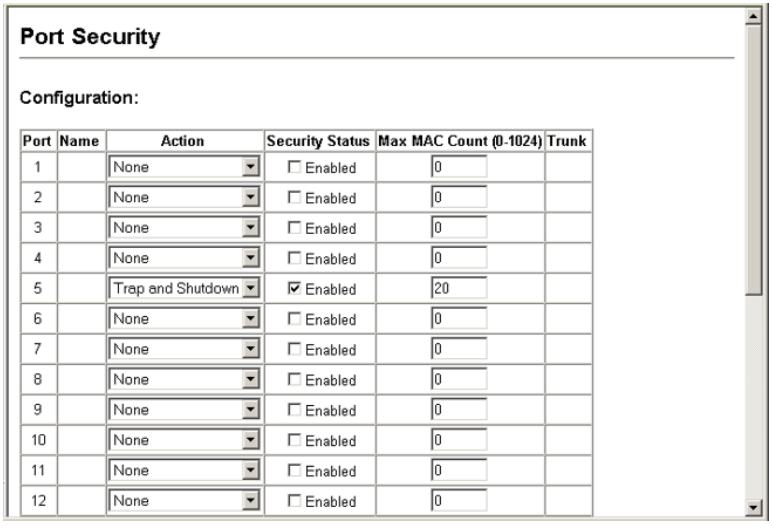

Port Security
Configuration:
Port Name Action Security Status Max MAC Count (0-1024) Trunk
1 None Enabled 0
2 None Enabled 0
3 None Enabled 0
4 None Enabled 0
5 Trap and Shutdown Enabled 20
6 None Enabled 0
7 None Enabled 0
8 None Enabled 0
9 None Enabled 0
10 None Enabled 0
11 None Enabled 0
12 None Enabled 0

Figure 3-39 Port Security

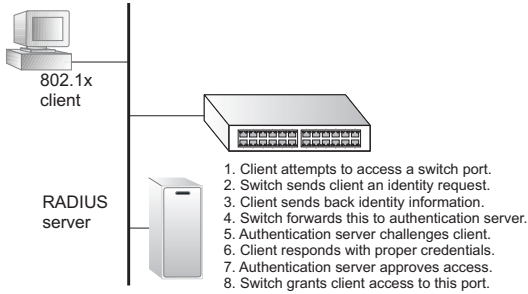
CLI – This example selects the target port, sets the port security action to send a trap and disable the port, specifies a maximum address count, and then enables port security for the port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown     4-102
Console(config-if)#port security max-mac-count 20
Console(config-if)#port security
Console(config-if)#
```

Configuring 802.1X Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.


802.1x client
RADIUS server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method must be MD5. (TLS, TTLS and PEAP will be supported in future releases.) The client responds to the appropriate method with its credentials, such as a password or certificate. The

RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1x "Auto" mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

Displaying 802.1X Global Settings

The 802.1X protocol provides port authentication.

Command Attributes

802.1X System Authentication Control – The global setting for 802.1X.

Web – Click Security, 802.1X, Information.



Figure 3-40 802.1X Global Information

CLI – This example shows the default global setting for 802.1X.

```
Console#show dot1x                                              4-110
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode              Authorized
1/1        disabled        Single-Host      ForceAuthorized     n/a
1/2        disabled        Single-Host      ForceAuthorized     n/a
:
802.1X Port Details

802.1X is disabled on port 1/1
:
802.1X is disabled on port 26
Console#
```

Configuring 802.1X Global Settings

The 802.1X protocol provides port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

Command Attributes

802.1X System Authentication Control – Sets the global setting for 802.1X. (Default: Disabled)

Web – Select Security, 802.1X, Configuration. Enable 802.1X globally for the switch, and click Apply.

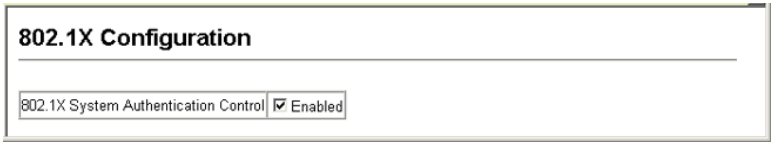


Figure 3-41 802.1X Global Configuration

CLI – This example enables 802.1X globally for the switch.

```
Console(config)#dot1x system-auth-control                       4-105
Console(config)#
```

Configuring Port Settings for 802.1X

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port. (Default: Disabled)
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host; Default: Single-Host)
- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **Max Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

- **Quiet Period** – Sets the time that a switch port waits after the Max Request count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1X, Port Configuration. Modify the parameters required, and click Apply.

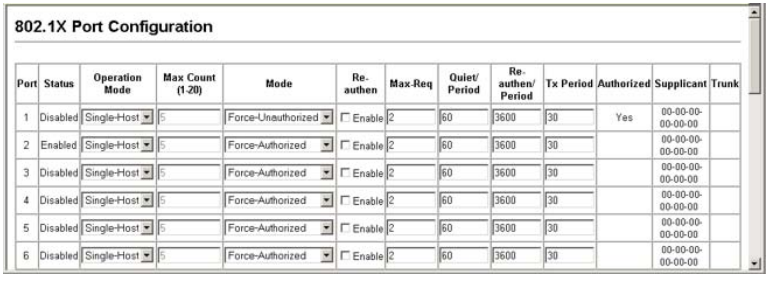

802.1X Port Configuration
Port
Status
Operation Mode
Max Count (1-20)
Mode
Re-authen
Max-Req
Quiet/ Period
Re-authen/ Period
Tx Period
Authorized
Supplicant
Trunk
1 Disabled Single-Host 5 Force-Unauthorized Enable 2 60 3600 30 Yes 00-00-00-00-00-00
2 Enabled Single-Host 5 Force-Authorized Enable 2 60 3600 30 00-00-00-00-00-00
3 Disabled Single-Host 5 Force-Authorized Enable 2 60 3600 30 00-00-00-00-00-00
4 Disabled Single-Host 5 Force-Authorized Enable 2 60 3600 30 00-00-00-00-00-00
5 Disabled Single-Host 5 Force-Authorized Enable 2 60 3600 30 00-00-00-00-00-00
6 Disabled Single-Host 5 Force-Authorized Enable 2 60 3600 30 00-00-00-00-00-00

Figure 3-42 802.1X Port Configuration

CLI – This example sets the 802.1X parameters on port 2. For a description of the additional fields displayed in this example, see "show dot1x" on page 4-110.

```
Console(config)#interface ethernet 1/2                          4-187
Console(config-if)#dot1x port-control auto                      4-106
Console(config-if)#dot1x re-authentication                      4-108
Console(config-if)#dot1x max-req 5                              4-105
Console(config-if)#dot1x timeout quiet-period 40                4-109
Console(config-if)#dot1x timeout re-authperiod 5                4-109
Console(config-if)#dot1x timeout tx-period 40                   4-110
Console(config-if)#end
Console#show dot1x                                              4-110

Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode              Authorized
1/1        disabled        Single-Host      ForceAuthorized     yes
1/2        enabled         Single-Host      Auto                yes
:
1/23       disabled        Single-Host      ForceAuthorized     n/a
1/24       disabled        Single-Host      ForceAuthorized     n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
reauth-enabled:       Disable
reauth-period:        3600
quiet-period:         60
tx-period:            30
supplicant-timeout:   30
server-timeout:       10
reauth-max:           2
max-req:              2
Status                Authorized
Operation mode        Single-Host
Max count             5
Port-control          Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    7

Authenticator State Machine
State                 Authenticated
Reauth Count          0

Backend State Machine
State                 Idle
Request Count         0
Identifier(Server)    6
```

```
Reauthentication State Machine
State                 Initialize
:
:
802.1X is disabled on port 1/24
Console#
```

Displaying 802.1X Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Table 3-7 802.1X Statistics

Parameter	Description
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

Table 3-7 802.1X Statistics (Continued)

Parameter	Description
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select Security, 802.1X, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.

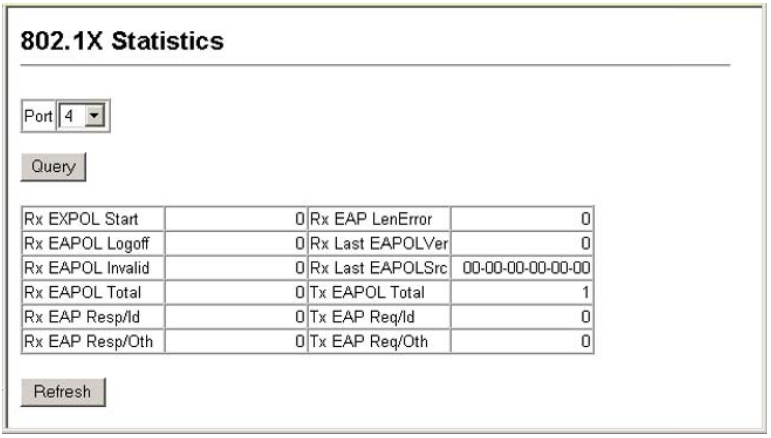


Figure 3-43 802.1X Port Statistics

CLI – This example displays the dot1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4          4-110

Eth 1/4
Rx: EAPOL      EAPOL      EAPOL      EAPOL      EAP       EAP       EAP
    Start     Logoff    Invalid    Total    Resp/Id  Resp/Oth LenError
        2          0          0       1007      672         0         0

    Last       Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL       EAP       EAP
    Total     Req/Id   Req/Oth
     2017     1005         0
Console#
```

Filtering IP Addresses for Management Access

You can create a list of up to 16 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

Command Usage

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **IP Filter List** – IP address which are allowed management access to this interface.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

Web – Click Security, IP Filter. Enter the IP addresses or range of addresses that are allowed management access to an interface, and click Add IP Filtering Entry.

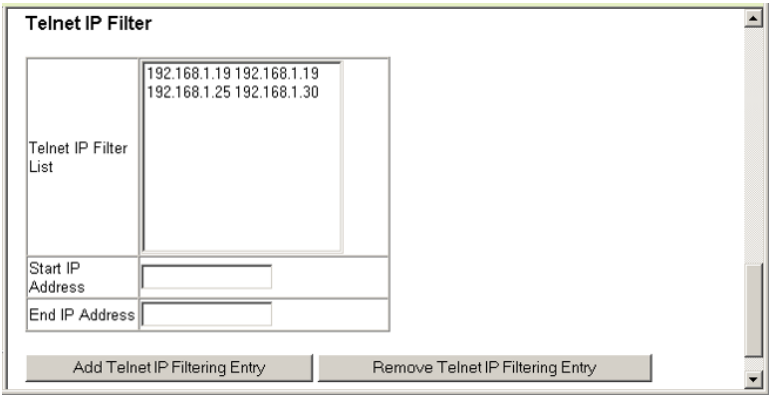


Figure 3-44 IP Filter

CLI – This example restricts management access for Telnet clients.

```
Console(config)#management telnet-client 192.168.1.19          4-38
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console(config)#exit
Console#show management all-client                              4-39
Management IP Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule. This is done by specifying masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
  - **Standard**: IP ACL mode that filters packets based on the source IP address.
  - **Extended**: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the "TCP" protocol is specified, then you can also filter packets based on the TCP control code.
  - **MAC**: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click Security, ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.



Figure 3-45 Selecting ACL Type

CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill                    4-117
Console(config-std-acl)#
```

Configuring a Standard IP ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **IP Address** – Source IP address.
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Then click Add.

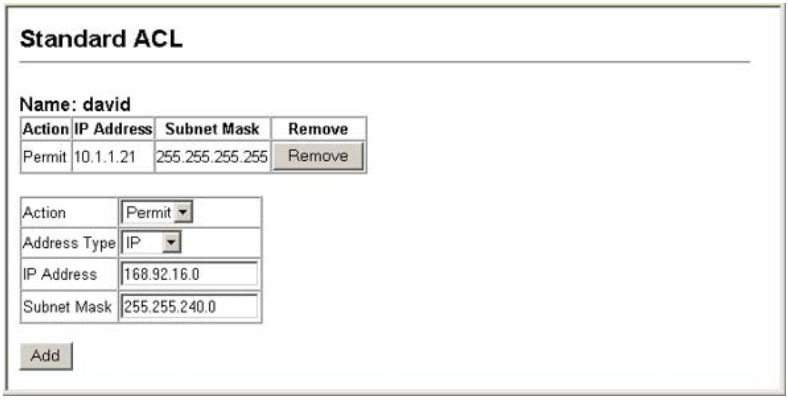


Figure 3-46 ACL Configuration - Standard IP

CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21                    4-118
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.

- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 3-105.)
- **Service Type** – Packet priority settings based on the following criteria:
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **TOS** – Type of Service level. (Range: 0-15)
  - **DSCP** – DSCP priority level. (Range: 0-63)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match. The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use control-code 2, control bitmask 2
  - Both SYN and ACK valid, use control-code 18, control bitmask 18
  - SYN valid and ACK invalid, use control-code 2, control bitmask 18

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.

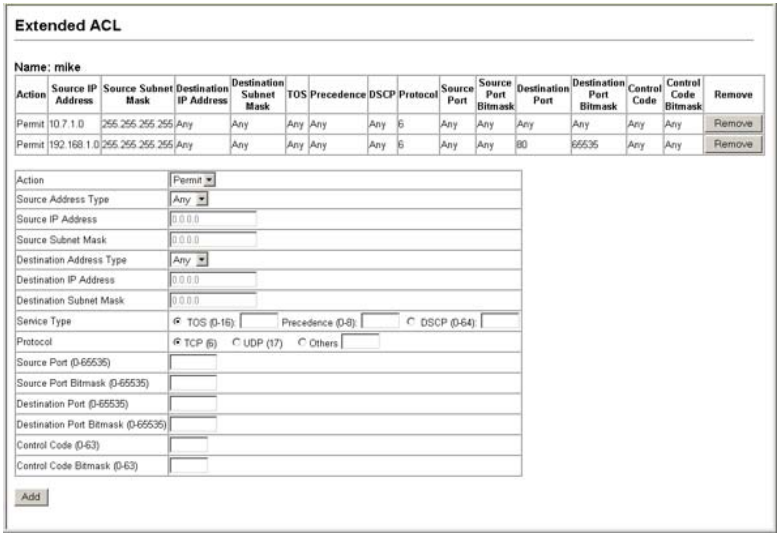


Figure 3-47 ACL Configuration - Extended IP

CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any     4-119
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0
  any destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0
  any control-flag 2 2
Console(config-std-acl)#
```

Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination** Address Type – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination MAC Bit Mask** – Hexidecimal mask for source or destination MAC address.
- **VID** – VLAN ID. (Range: 1-4093)
- **VID Bit Mask** – VLAN bitmask. (Range: 1-4093)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bit Mask** – Protocol bitmask. (Range: 600-fff hex.)
- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **Tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Command Usage

Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexidecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.

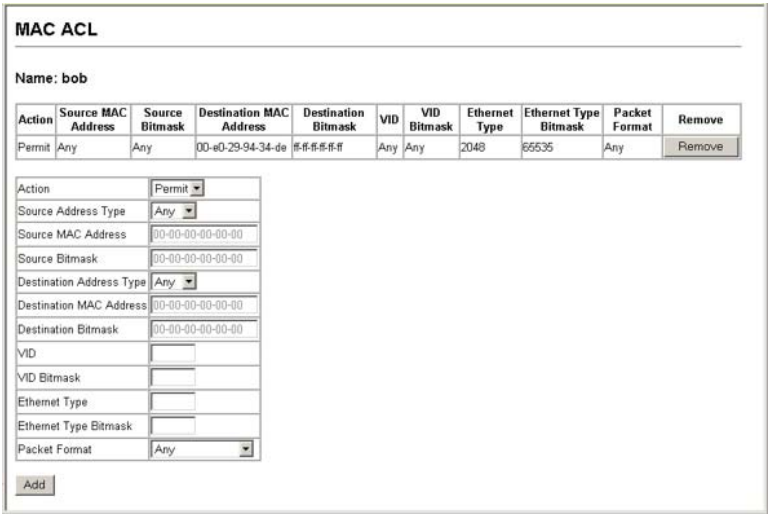


Figure 3-48 ACL Configuration - MAC

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
  ethertype 0800                                          4-130
Console(config-mac-acl)#
```

Configuring ACL Masks

You must specify masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Usage

- Up to seven entries can be assigned to an ACL mask.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- First create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Specifying the Mask Type

Use the ACL Mask Configuration page to edit the mask for the Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL.

Web – Click Security, ACL, Mask Configuration. Click Edit for one of the basic mask types to open the configuration page.

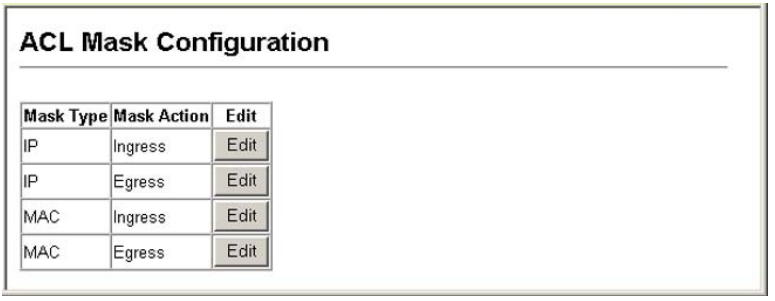


Figure 3-49 Selecting ACL Mask Types

CLI – This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in              4-122
Console(config-ip-mask-acl)#mask host any                      4-123
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Command Usage

Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to match any address, "Host" to specify a host address (not a subnet), or "IP" to specify a range of addresses. (Options: Any, Host, IP; Default: Any)
- **Source/Destination Subnet Mask** – Source or destination address of rule must match this bitmask. (See the description for SubMask on page 3-105.)
- **Protocol Mask** – Check the protocol field.
- **Service Type Mask** – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)
- **Source/Destination Port Bit Mask** – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **Control Code Bit Mask** – Control flags of rule must match this bitmask. (Range: 0-63)

Web – Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.

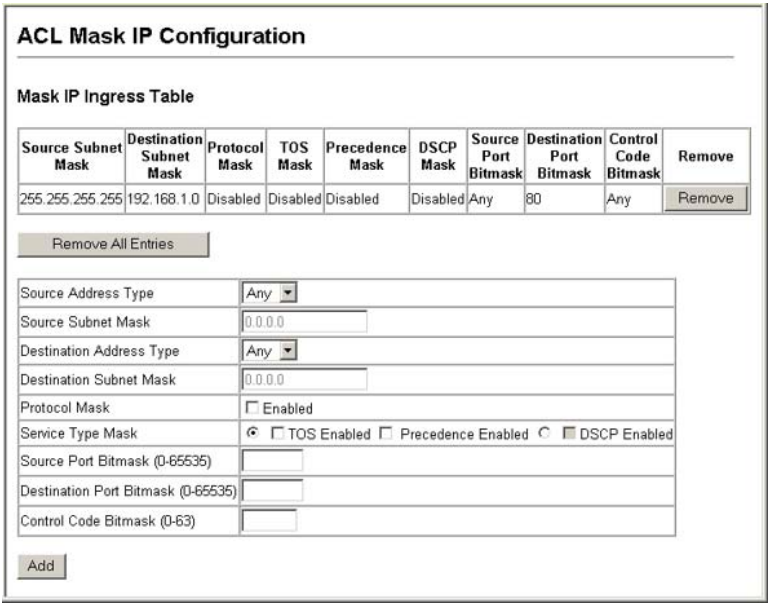


Figure 3-50 ACL Mask Configuration - IP

CLI – This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the "deny 10.1.1.1 255.255.255.255" rule has the higher precedence according the "mask host any" entry.

```
Console(config)#access-list ip standard A2                    4-117
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0         4-118
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in             4-122
Console(config-ip-mask-acl)#mask host any                     4-123
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Command Usage

You must configure a mask for an ACL rule before you can bind it to a port.

Command Attributes

- **Source/Destination Address Type** – Use "Any" to match any address, "Host" to specify the host address for a single node, or "MAC" to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination Bit Mask** – Address of rule must match this bitmask.
- **VID Bitmask** – VLAN ID of rule must match this bitmask.
- **Ethernet Type Bit Mask** – Ethernet type of rule must match this bitmask.
- **Packet Format Mask** – A packet format must be specified in the rule.

Web – Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for specific VLAN ID(s) or Ethernet type(s). Or check for rules where a packet format was specified. Then click Add.

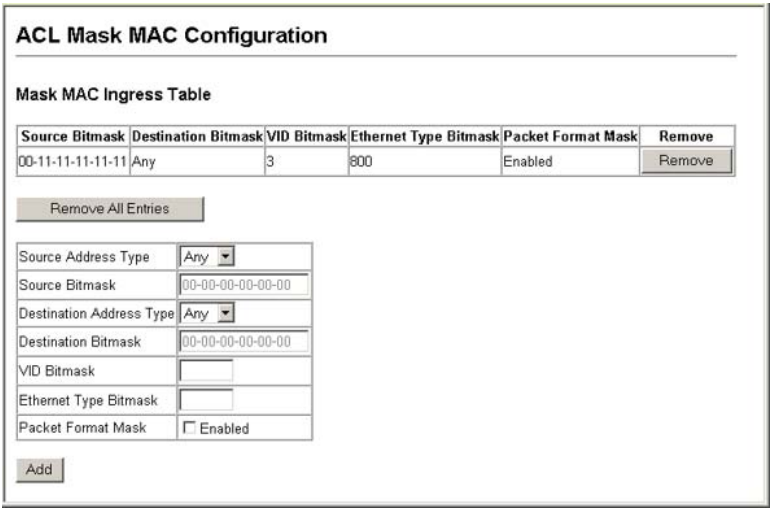


Figure 3-51 ACL Mask Configuration - MAC

CLI – This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4                                  4-129
Console(config-mac-acl)#permit any any                              4-130
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
  ff-ff-ff-ff-ff-ff any vid 3                                       4-130
Console(config-mac-acl)#end
Console#show access-list                                            4-137
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in                  4-132
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff
  any vid                                                           4-133
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12                             4-187
Console(config-if)#mac access-group M4 in                           4-136
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you should bind them to the ports that need to filter traffic. You can only bind a port to one ACL for each basic type – IP ingress, IP egress, MAC ingress and MAC egress.

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port.
- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.

- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

- **Port** – Fixed port or SFP module. (Range: 1-24)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IN** – ACL for ingress packets.
- **OUT** – ACL for egress packets.
- *ACL Name* – Name of the ACL.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress or egress traffic, select the required ACL from the drop-down list, then click Apply.

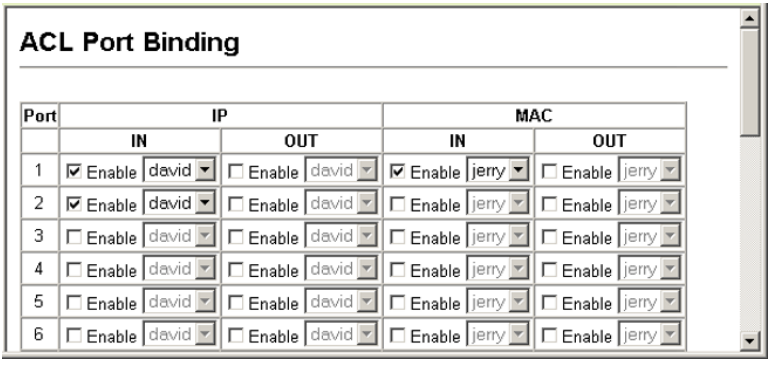

ACL Port Binding
Port
IP
MAC
IN
OUT
IN
OUT
1 Enable david Enable david Enable jerry Enable jerry
2 Enable david Enable david Enable jerry Enable jerry
3 Enable david Enable david Enable jerry Enable jerry
4 Enable david Enable david Enable jerry Enable jerry
5 Enable david Enable david Enable jerry Enable jerry
6 Enable david Enable david Enable jerry Enable jerry

Figure 3-52 ACL Port Binding

CLI – This examples assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1                          4-187
Console(config-if)#ip access-group david in                     4-127
Console(config-if)#mac access-group jerry in                    4-136
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

Port Configuration

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, and auto-negotiation.

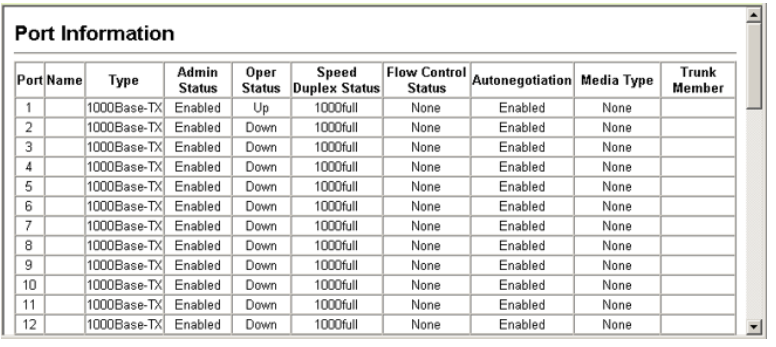
Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type. (1000BASE-T, SFP, or 10GBASE-LR)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Flow Control Status**[5] – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Media Type**[6] – Shows the forced/preferred port type to use for combination ports 21-24. (Copper-Forced, SFP-Forced, SFP-Preferred-Auto)
- **Trunk Member** – Shows if port is a trunk member.

5. There are interoperability problems between Flow Control and Head-of-Line (HOL) blocking for the switch ASIC; Flow Control is therefore not supported for this switch.
6. Port Information only.

- **Creation**[7] – Shows if a trunk is manually configured or dynamically set via LACP.

Web – Click Port, Port Information or Trunk Information.



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1		1000Base-TX	Enabled	Up	1000full	None	Enabled	None	
2		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
3		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
4		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
5		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
6		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
7		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
8		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
9		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
10		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
11		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
12		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	

Figure 3-53 Port - Port Information

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (1000BASE-T, SFP, or 10GBASE-LR)
- **MAC address** – The physical layer address for this port. (To access this item on the web, see "Setting the Switch's IP Address" on page 3-22.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see

7. Trunk Information only.

"Configuring Interface Connections" on page 3-48.) The following capabilities are supported.

- **10half** - Supports 10 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **1000full** - Supports 1000 Mbps full-duplex operation
- **10Gfull** - Supports 10 Gbps full-duplex operation

- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast storm limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow control**[8] – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port security** – Shows if port security is enabled or disabled.
- **Max MAC count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 1024 addresses)
- **Port security action** – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)
- **Media type** – Shows the forced/preferred port type to use for combination ports 21-24 (SMC8724ML3) or 45-48 (SMC8748ML3). (copper forced, SFP forced, SFP preferred auto)

Current status:

- **Link status** – Indicates if the link is up or down.
- **Port operation status** – Provides detailed information on port state. (Displayed only when the link is up.).
- **Operation speed-duplex** – Shows the current speed and duplex mode.
- **Flow control type** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or none)

8. There are interoperability problems between Flow Control and Head-of-Line (HOL) blocking for the switch ASIC; Flow Control is therefore not supported for this switch.

CLI – This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/5                    4-196
Information of Eth 1/13
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A5
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full,
1000full
  Broadcast storm:        Enabled
  Broadcast storm limit:  500 packets/second
  Flow control:           Disabled
  LACP:                   Disabled
  Port security:          Disabled
  Max MAC count:          0
  Port security action:   None
  Media type:             None
 Current status:
  Link status:            Down
  Operation speed-duplex: 1000full
  Flow control type:      None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed and duplex mode.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode (i.e., with auto-negotiation disabled).
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you

can force the settings for speed and mode.The following capabilities are supported.

- **10half** - Supports 10 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **1000full** - Supports 1 Gbps full-duplex operation
- **10Gfull** - Supports 10 Gbps full-duplex operation

(Default: Autonegotiation enabled; Advertised capabilities for RJ-45: 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; SFP: 1000BASE-SX/LX/LH – 1000full; 10G Modules: 10GBASE-LR – 10Gfull)

- **Media Type** – Shows the forced/preferred port type to use for the combination ports. (SMC8724ML3: Ports 21-24; SMC8748ML3: Ports 45-48)
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port (even if module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see "Creating Trunk Groups" on page 3-125.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.

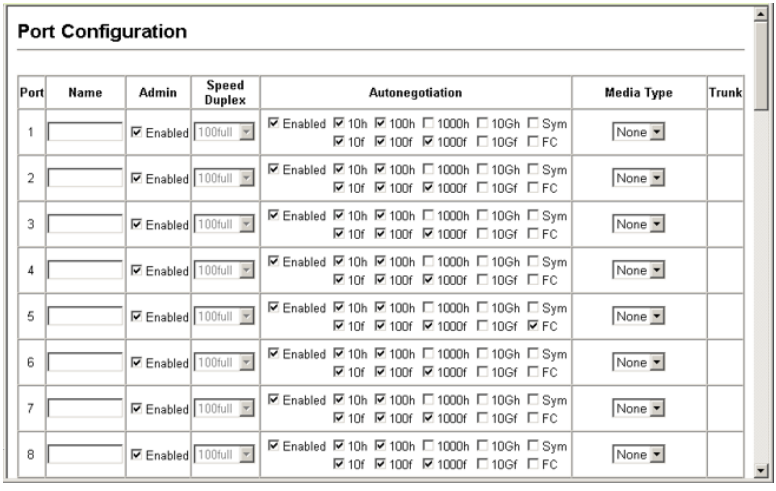


Figure 3-54 Port - Port Configuration

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                    4-187
Console(config-if)#description RD SW#13                    4-187
Console(config-if)#shutdown                                4-193
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                          4-189
Console(config-if)#speed-duplex 100half                    4-188
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                    4-190
Console(config-if)#capabilities 100full
Console(config-if)#exit
Console(config)#interface ethernet 1/21
Console(config-if)#media-type copper-forced                4-192
Console(config-if)#
```

Creating Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices (i.e., single switch or a stack). You can create up to 32 trunks.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

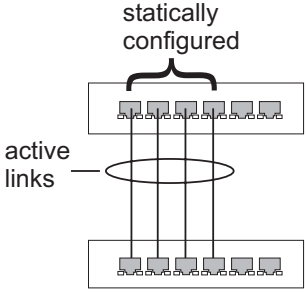
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 32 trunks on a switch or stack, with up to eight Gigabit ports per trunk or up to four 10Gbps ports per trunk. Note that because the stack functions conceptually as a single system, you can include ports from different units in the same trunk. For example, you could connect ports spread across several units that belong VLAN 2 into a common trunk.

- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Statically Configuring a Trunk

Command Usage



- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

Command Attributes

- **Member List** (Current) – Shows configured trunks (Trunk ID, Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Trunk** – Trunk identifier. (Range: 1-32)
  - **Unit** – Stack unit. (Range: 1-8)
  - **Port** – Port identifier. (Range: 1-25/49)

Web – Click Port, Trunk Membership. Enter a trunk ID of 1-32 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.

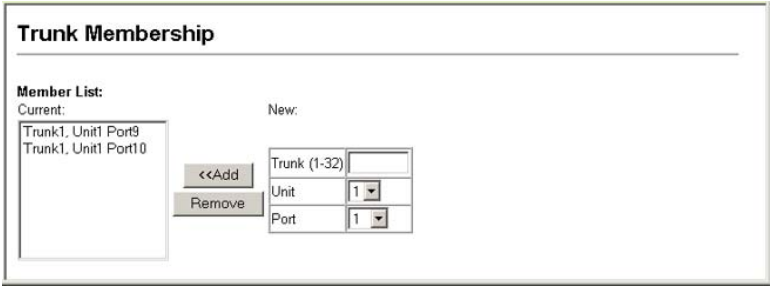


Figure 3-55 Static Trunk Configuration

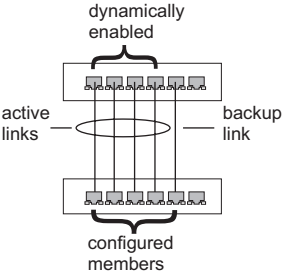
CLI – This example creates trunk 1 with ports 9 and 10. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1                          4-187
Console(config-if)#exit
Console(config)#interface ethernet 1/9                            4-187
Console(config-if)#channel-group 1                                4-206
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                     4-196
Information of Trunk 1
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A2
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full,
1000full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             User
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 1000full
  Flow control type:      None
  Member Ports: Eth1/9, Eth1/10,
Console#
```

Enabling LACP on Selected Ports

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.



- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- Trunks dynamically established through LACP will also be shown in the Member List on the Trunk Membership menu (see page 3-126).

Command Attributes

- **Member List** (Current) – Shows configured trunks (Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Unit** – Stack unit. (Range: 1-8)
  - **Port** – Port identifier. (Range: 1-25/49)

Web – Click Port, LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.

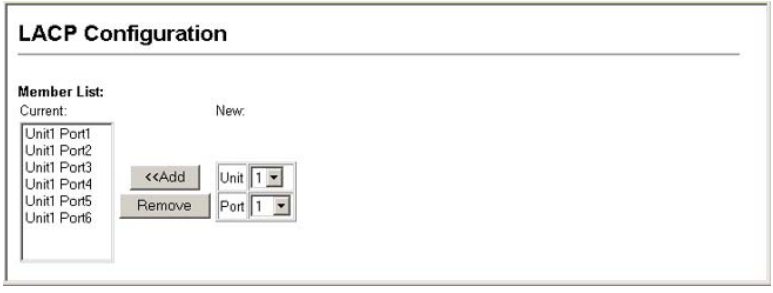


Figure 3-56 LACP Trunk Configuration

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/1                          4-187
Console(config-if)#lacp                                         4-206
Console(config-if)#exit
:
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                   4-196
Information of Trunk 1
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A2
 Configuration:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full,
1000full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             LACP
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 1000full
  Flow control type:      None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

Configuring LACP Parameters

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the "port channel" Admin Key is set (page 4-142), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

  Note – If the port channel admin key (lacp admin key, page 4-210) is not set (through the CLI) when a channel group is formed (i.e., it has a null value

of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 4-209).

Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; i.e., the ports on this switch.

- **Port** – Port number. (Range: 1-25/49)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
  - Ports must be configured with the same system priority to join the same LAG.
  - System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.

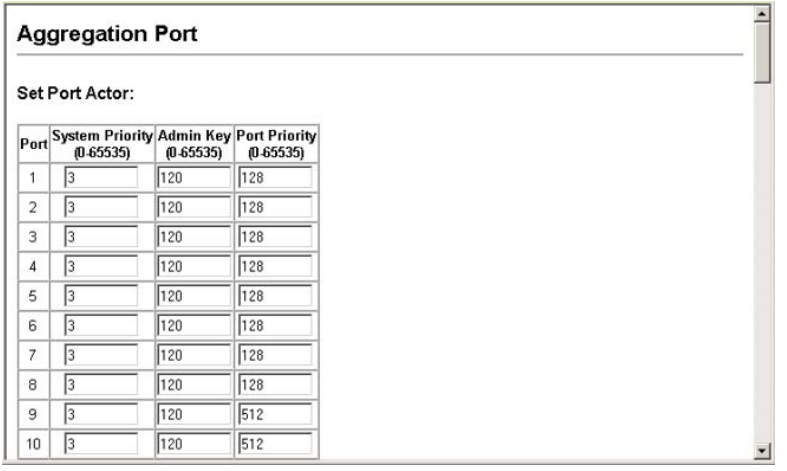


Figure 3-57 LACP - Aggregation Port

CLI – The following example configures LACP parameters for ports 1-10. Ports 1-8 are used as active members of the LAG, ports 9 and 10 are set to backup mode.

```
Console(config)#interface ethernet 1/1                          4-187
Console(config-if)#lacp actor system-priority 3                 4-208
Console(config-if)#lacp actor admin-key 120                     4-209
Console(config-if)#lacp actor port-priority 128                 4-211
Console(config-if)#exit
:
Console(config)#interface ethernet 1/10
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid                                         4-212
Channel Group    System Priority    System MAC Address
---------------------------------------------------------------------
           1                  3     00-00-E9-31-31-31
           2              32768     00-00-E9-31-31-31
           3              32768     00-00-E9-31-31-31
:
Console#show lacp 1 internal                                    4-212
Port channel: 1
---------------------------------------------------------------------
Oper Key:  120
Admin Key: 0
Eth 1/ 1
---------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 3
  LACP Port Priority:   128
  Admin Key:            120
  Oper Key:             120
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
```

Displaying LACP Port Counters

You can display statistics for LACP protocol messages.

Table 3-8 LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received by this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Web – Click Port, LACP, Port Counters Information. Select a member port to display the corresponding information.

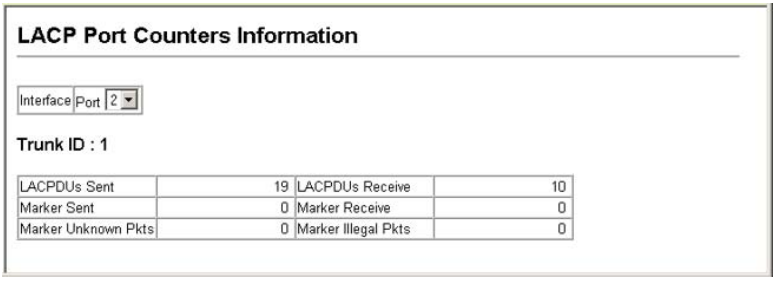

LACP Port Counters Information
Interface Port 2
Trunk ID : 1
LACPDUs Sent 19 LACPDUs Receive 10
Marker Sent 0 Marker Receive 0
Marker Unknown Pkts 0 Marker Illegal Pkts 0

Figure 3-58 LACP - Port Counters Information

CLI – The following example displays LACP counters for port channel 1.

```
Console#show lacp 1 counters                                    4-212
Port channel: 1
-------------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------------
  LACPDUs Sent:          19
  LACPDUs Receive:       10
  Marker Sent:           0
  Marker Receive:        0
  LACPDUs Unknown Pkts:  0
  LACPDUs Illegal Pkts:  0
:
```

Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

Table 3-9 LACP Internal Configuration Information

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

Table 3-9 LACP Internal Configuration Information (Continued)

Field	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.

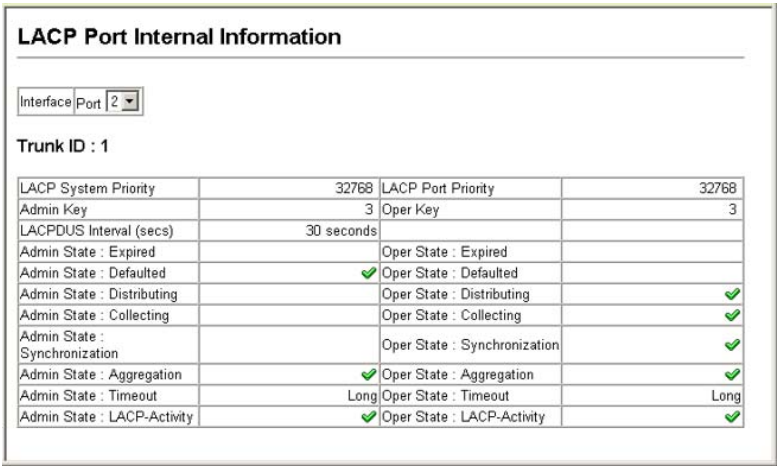

LACP Port Internal Information
Interface Port 2
Trunk ID : 1
LACP System Priority 32768 LACP Port Priority 32768
Admin Key 3 Oper Key 3
LACPDUS Interval (secs) 30 seconds
Admin State : Expired Oper State : Expired
Admin State : Defaulted Oper State : Defaulted
Admin State : Distributing Oper State : Distributing
Admin State : Collecting Oper State : Collecting
Admin State : Synchronization Oper State : Synchronization
Admin State : Aggregation Oper State : Aggregation
Admin State : Timeout Long Oper State : Timeout Long
Admin State : LACP-Activity Oper State : LACP-Activity

Figure 3-59 LACP - Port Internal Information

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show lacp 1 internal                                    4-212
Port channel: 1
------------------------------------------------------------------------
Oper Key:  3
Admin Key: 0
Eth 1/ 2
------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 32768
  LACP Port Priority:   32768
  Admin Key:            3
  Oper Key:             3
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
⋮
```

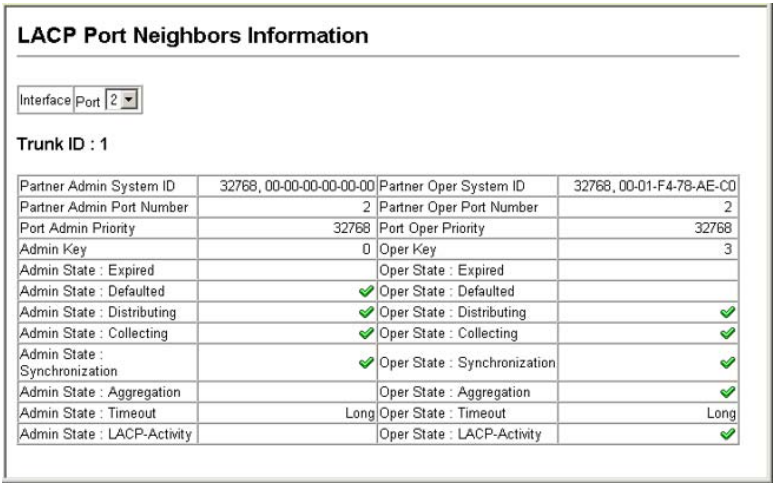
Displaying LACP Settings and Status for the Remote Side

You can display configuration settings and the operational state for the remote side of an link aggregation.

Table 3-10 LACP Neighbor Configuration Information

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Interface Port 2

Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-01-F4-78-AE-C0
Partner Admin Port Number	2	Partner Oper Port Number	2
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	3
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✔	Oper State : Defaulted	
Admin State : Distributing	✔	Oper State : Distributing	✔
Admin State : Collecting	✔	Oper State : Collecting	✔
Admin State : Synchronization	✔	Oper State : Synchronization	✔
Admin State : Aggregation		Oper State : Aggregation	✔
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✔

Figure 3-60 LACP - Port Neighbors Information

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show lacp 1 neighbors                                    4-212
Port channel 1 neighbors
---------------------------------------------------------------------
Eth 1/2
---------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    32768, 00-01-F4-78-AE-C0
  Partner Admin Port Number: 2
  Partner Oper Port Number:  2
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:              distributing, collecting, synchronization,
                           aggregation, long timeout, LACP-activity
⋮
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

- Broadcast control does not effect IP multicast traffic.
- The resolution for Gigabit ports is 1 packet per second (pps); i.e., any setting between 500-262143 is acceptable. However, the resolution for the 10 Gigabit port is in steps of 1041 pps.

Command Attributes

- **Port**[9] – Port number.
- **Trunk**[10] – Trunk number
- **Type** – Indicates the port type. (1000BASE-T, SFP, or 10GBASE-LR)
- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (1000BASE Options: 500-262143 packets per second; Default: 500 pps, 10GBASE Options: 1041-262143 packets per second; Default: 1041 pps)
- **Trunk** – Shows if port is a trunk member.

9. Port Broadcast Control
10. Trunk Broadcast Control

Web – Click Port, Port Broadcast Control or Trunk Broadcast Control. Check the Enabled box for any interface, set the threshold, and click Apply.

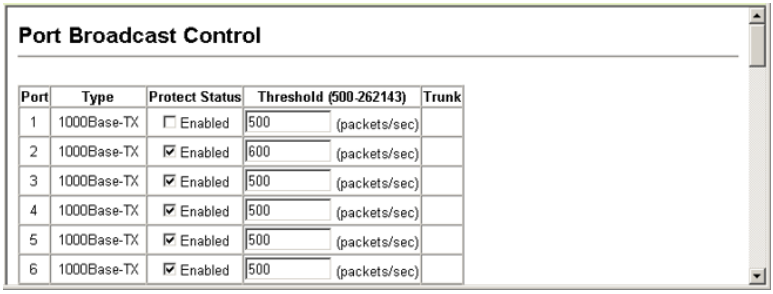


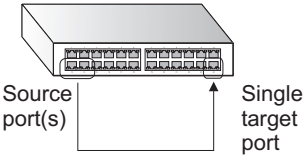
Figure 3-61 Port Broadcast Control

CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.

```
Console(config)#interface ethernet 1/1                          4-187
Console(config-if)#no switchport broadcast                      4-194
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 600         4-194
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2                 4-199
Information of Eth 1/2
 Broadcast threshold:           Enabled, 600 packets/second
 LACP status:                   Disabled
 Ingress rate limit:            Disable, 1000M bits per second
 Egress rate limit:             Disable, 1000M bits per second
 VLAN membership mode:          Hybrid
 Ingress rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 GVRP status:                   Disabled
 Allowed VLAN:                  1(u),
 Forbidden VLAN:
Console#
```

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Unit** – The unit whose port traffic will be monitored. (Range: 1-8)
- **Source Port** – The port whose traffic will be monitored. (Range: 1-25/49)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)
- **Target Unit** – The unit whose port will "duplicate" or "mirror" the traffic on the source port. (Range: 1-8)
- **Target Port** – The port that will "mirror" the traffic from the source port. (Range: 1-25/49)

Web – Click Port, Mirror Port Configuration. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.

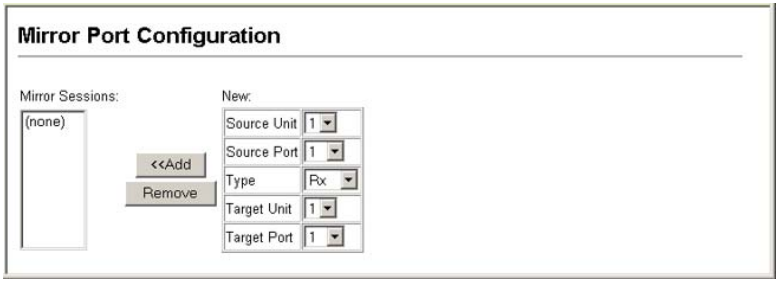


Figure 3-62 Mirror Port Configuration

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10                    4-187
Console(config-if)#port monitor ethernet 1/13              4-201
Console(config-if)#
```

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attribute

Rate Limit – Sets the output rate limit for an interface.

- Default Status – Disabled
- Default Rate – Gigabit Ethernet: 1000 Mbps;
  10 Gigabit Ethernet: 10000 Mbps
- Range – Gigabit Ethernet: 1 - 1000 Mbps;
  10 Gigabit Ethernet: 1 - 10000 Mbps

Web - Click Port, Rate Limit, Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.

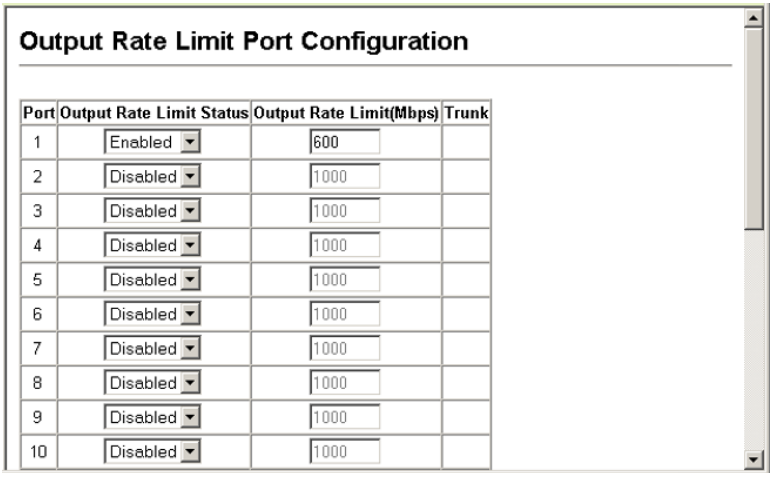


Figure 3-63 Rate Limit Configuration

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 600 Mbps.

```
Console(config)#interface ethernet 1/1                    4-187
Console(config-if)#rate-limit input 600                   4-203
Console(config-if)#rate-limit output 600
Console(config-if)#
```

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated

since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as HP OpenView.

Table 3-11 Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Table 3-11 Port Statistics (Continued)

Parameter	Description
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.

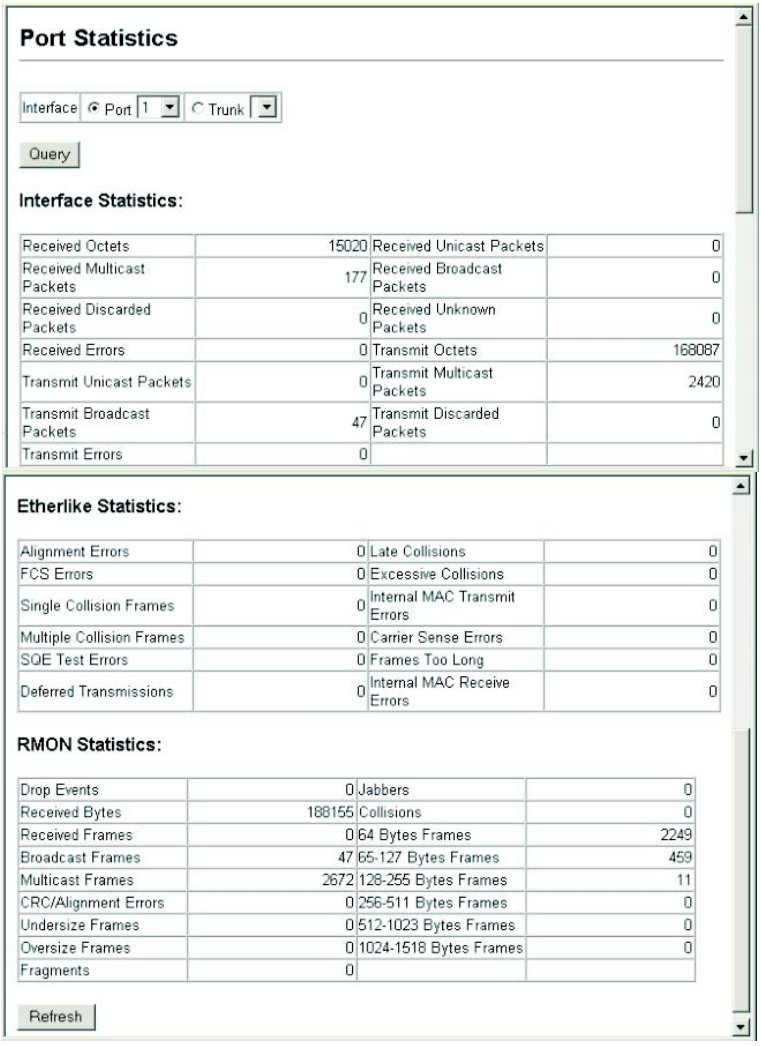
Table 3-11 Port Statistics (Continued)

Parameter	Description
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 3-11 Port Statistics (Continued)

Parameter	Description
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Port, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.



Port Statistics

Interface: Port 1 / Trunk

Query

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

Figure 3-64 Port Statistics

CLI – This example shows statistics for port 12.

```
Console#show interfaces counters ethernet 1/12                    4-197
Ethernet 1/12
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts**[11] – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4093).

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.

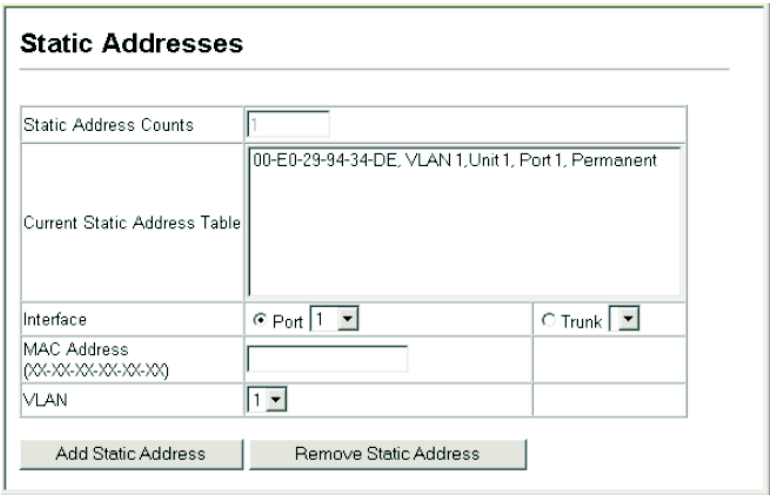


Figure 3-65 Static Addresses

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
  interface ethernet 1/1 vlan 1 delete-on-reset              4-217
Console(config)#
```

11. Web Only.

Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Address Table Sort Key** – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.

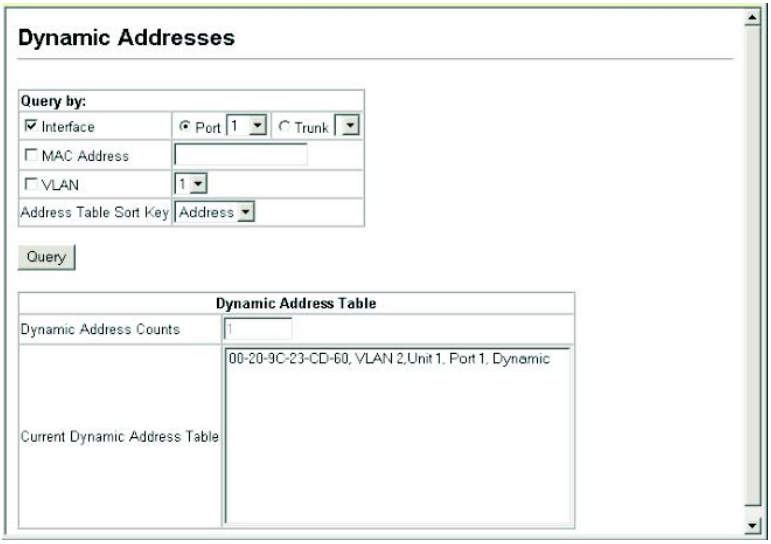


Figure 3-66 Dynamic Addresses

CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1        4-219
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- **Aging Status** – Enables/disables the aging function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.

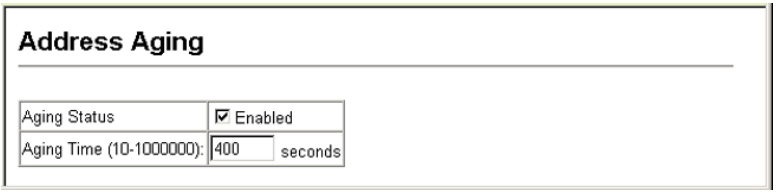


Figure 3-67 Address Aging

CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400                4-220
Console(config)#
```

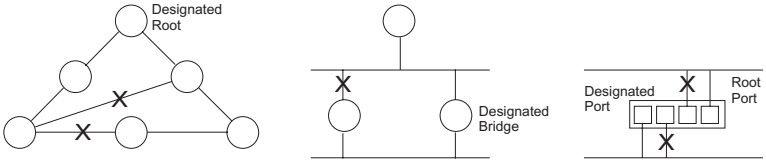
Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves must faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports

start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (an extension of RSTP) is designed to support independent spanning trees based on VLAN groups. Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree mode is set to MSTP (page 3-161), and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
  - **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
  - **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

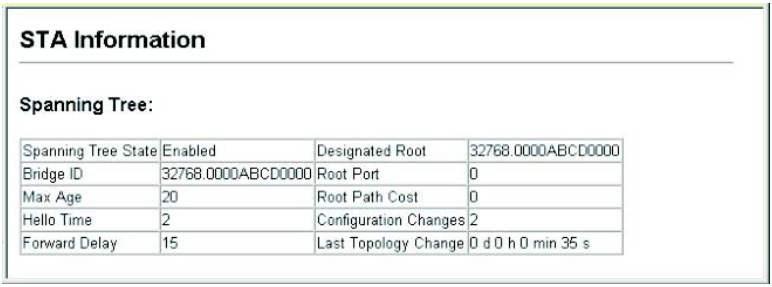
These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D)
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- **Instance** – Instance identifier of this spanning tree. (This is always 0 for the CIST.)
- **VLANs configuration** – VLANs assigned to the CIST.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices

have the same priority, the device with the lowest MAC address will then become the root device.

- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)
- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Max hops** – The max number of hop counts for the MST region.
- **Remaining hops** – The remaining number of hop counts for the MST instance.
- **Transmission limit** – The minimum interval between the transmission of consecutive RSTP/MSTP BPDUs.
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

Figure 3-68 STA Information

CLI – This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree                                          4-243
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode:                MSTP
 Spanning tree enable/disable:      enable
 Instance:                          0
 Vlans configuration:               1-4093
 Priority:                          32768
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Max hops:                          20
 Remaining hops:                    20
 Designated Root                    32768.0.0000ABCD0000
 Current root port:                 1
 Current root cost                  200000
 Number of topology changes:        1
 Last topology changes time (sec.): 13380
 Transmission limit:                3
 Path Cost Method:                  long
```

```
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status:             enabled
 Role:                     disable
 State:                    discarding
 External admin path cost: 10000
 Internal admin cost:      10000
 External oper path cost:  10000
 Internal oper path cost:  10000
 Priority:                 128
 Designated cost:          300000
 Designated port:          128.1
 Designated root:          32768.0000E8AAAA00
 Designated bridge:        32768.0030F1D473A0
 Fast forwarding:          disabled
 Forward transitions:      0
 Admin edge port:          disabled
 Oper edge port:           disabled
 Admin Link type:          auto
 Oper Link type:           point-to-point
 Spanning Tree Status:     enabled
:
:
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol[12]

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

12. STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

- Rapid Spanning Tree Protocol
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
- Multiple Spanning Tree Protocol
  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).

- **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
- **MSTP**: Multiple Spanning Tree (IEEE 802.1s)

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - Default: 32768
  - Range: 0-61440, in steps of 4096
    - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each

port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- Default: 15
- Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
- Maximum: 30

Configuration Settings for RSTP

The following attributes apply to both RSTP and MSTP:

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Configuration Settings for MSTP

- **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned. (Default: 65)
- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- **Region Revision**[13] – The revision for this MSTI. (Range: 0-65535; Default: 0)
- **Region Name** – The name for this MSTI. (Maximum length: 32 characters)
- **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

13. The MST name and revision number are both required to uniquely identify an MST region.

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, and click Apply.

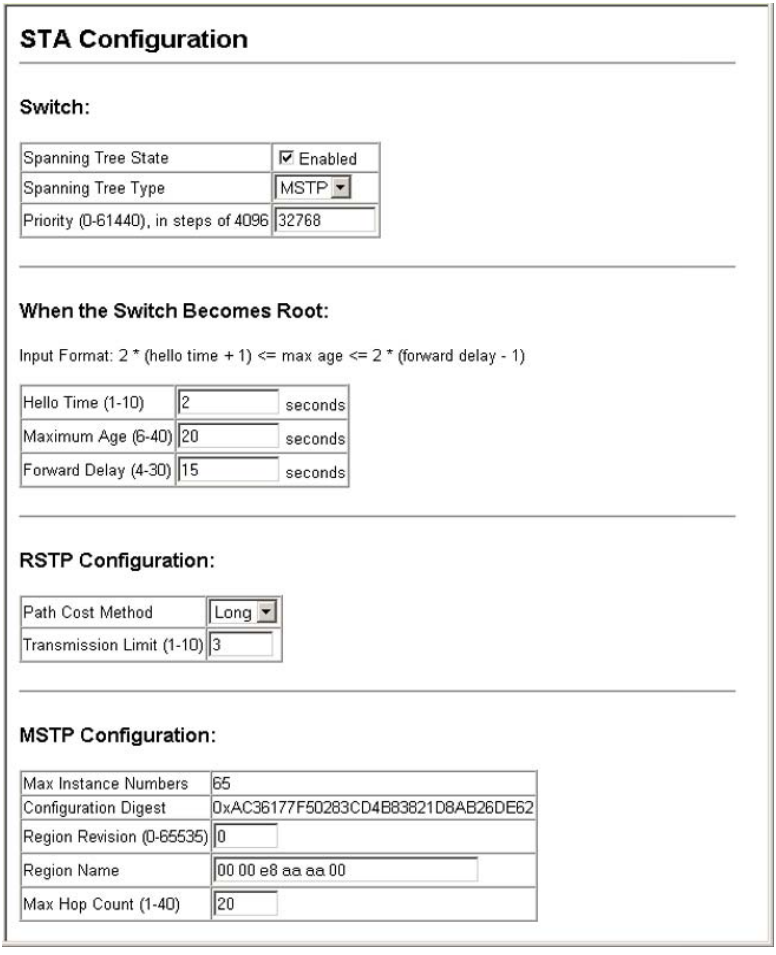


Figure 3-69 STA Global Configuration

CLI – This example enables Spanning Tree Protocol, sets the mode to MST, and then configures the STA and MSTP parameters.

```
Console(config)#spanning-tree                                    4-222
Console(config)#spanning-tree mode mstp                          4-223
Console(config)#spanning-tree priority 40000                     4-227
Console(config)#spanning-tree hello-time 5                       4-226
Console(config)#spanning-tree max-age 38                         4-226
Console(config)#spanning-tree forward-time 20                    4-225
Console(config)#spanning-tree pathcost method long               4-228
Console(config)#spanning-tree transmission-limit 4               4-229
Console(config)#Console(config)#spanning-tree
 mst-configuration                                               4-229
Console(config-mstp)#revision 1                                  4-233
Console(config-mstp)#name R&D                                    4-232
Console(config-mstp)#max-hops 30                                 4-233
Console(config-mstp)#
```

Displaying Interface Settings

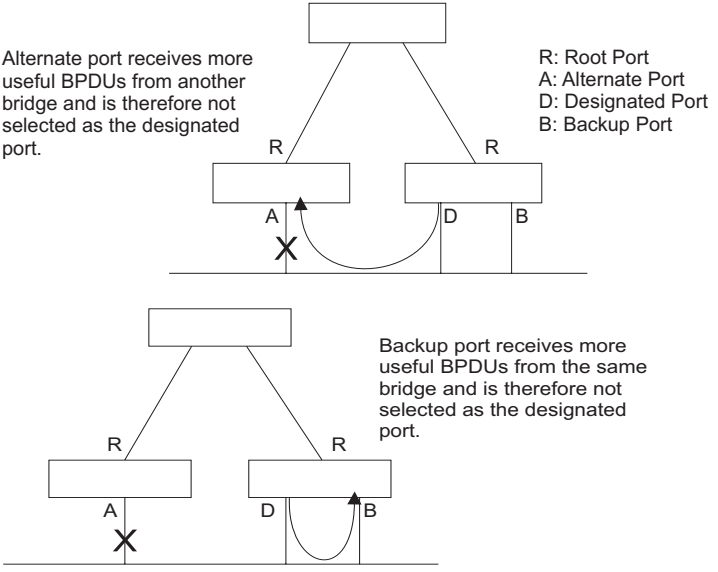
The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

Field Attributes

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

    The rules defining port status are:
    - A port on a network segment with no other STA compliant bridging device is always forwarding.

  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 3-170.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 3-170 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), or is the MSTI regional root (i.e., **master** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.



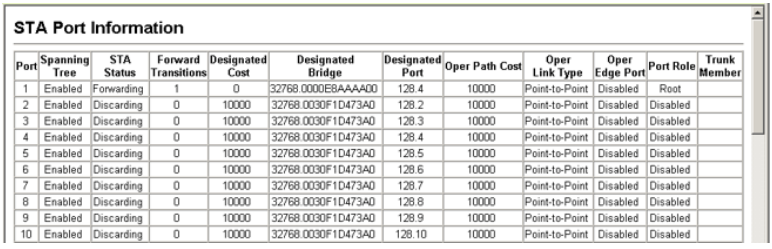
- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- **External path cost** – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Internal path cost** – The path cost for the MST. See the preceding item.
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA, Port Information or STA Trunk Information.



STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	1	0	32768.0000E8AAAA00	128.4	10000	Point-to-Point	Disabled	Root	
2	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.2	10000	Point-to-Point	Disabled	Disabled	
3	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.4	10000	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.5	10000	Point-to-Point	Disabled	Disabled	
6	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.6	10000	Point-to-Point	Disabled	Disabled	
7	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.7	10000	Point-to-Point	Disabled	Disabled	
8	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.8	10000	Point-to-Point	Disabled	Disabled	
9	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.9	10000	Point-to-Point	Disabled	Disabled	
10	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.10	10000	Point-to-Point	Disabled	Disabled	

Figure 3-70 STA Port Information

CLI – This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/5                          4-243
Eth  1/ 5 information
---------------------------------------------------------------
 Admin status:             enabled
 Role:                     disable
 State:                    discarding
 External admin path cost: 10000
 Internal admin cost:      10000
 External oper path cost:  10000
 Internal oper path cost:  10000
 Priority:                 128
 Designated cost:          10000
 Designated port:          128.1
 Designated root:          32768.0.0000E8AAAA00
 Designated bridge:        32768.0.0030F1D473A0
 Fast forwarding:          disabled
 Forward transitions:      2
 Admin edge port:          disabled
 Oper edge port:           disabled
 Admin Link type:          auto
 Oper Link type:           point-to-point
 Spanning Tree Status:     enabled

Console#
```

Configuring Interface Settings

You can configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 3-166 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.

  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk**[14] – Indicates if a port is a member of a trunk.

The following interface attributes can be configured:

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

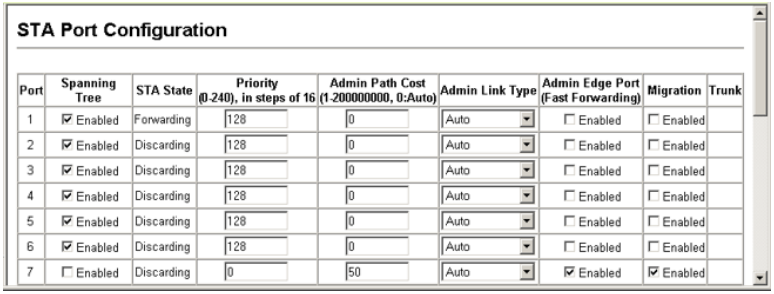
14. STA Port Configuration only

- Range –
  - Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000
  - 10 Gigabit Ethernet: 200-20,000
- Default –
  - Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
  - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
  - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000
  - 10 Gigabit Ethernet – Full duplex: 1000; trunk: 500

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port** (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually

re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Web – Click Spanning Tree, STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.



STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Admin Path Cost (1-200000000, 0:Auto)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	Enabled	Forwarding	128	0	Auto	Enabled	Enabled	
2	Enabled	Discarding	128	0	Auto	Enabled	Enabled	
3	Enabled	Discarding	128	0	Auto	Enabled	Enabled	
4	Enabled	Discarding	128	0	Auto	Enabled	Enabled	
5	Enabled	Discarding	128	0	Auto	Enabled	Enabled	
6	Enabled	Discarding	128	0	Auto	Enabled	Enabled	
7	Enabled	Discarding	0	50	Auto	Enabled	Enabled	

Figure 3-71 STA Port Configuration

CLI – This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7                    4-187
Console(config-if)#no spanning-tree spanning-disabled     4-234
Console(config-if)#spanning-tree port-priority 0          4-236
Console(config-if)#spanning-tree cost 50                  4-235
Console(config-if)#spanning-tree link-type auto           4-239
Console(config-if)#no spanning-tree edge-port             4-237
Console(config-if)#spanning-tree protocol-migration       4-242
```

Configuring Multiple Spanning Trees

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 65 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region

(page 3-164) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (STA Configuration, page 3-161).
2. Enter the spanning tree priority for the selected MST instance (MSTP VLAN Configuration).
3. Add the VLANs that will share this MSTI (MSTP VLAN Configuration).

Note: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

Command Attributes

- **MST Instance** – Instance identifier of this spanning tree. (Default: 0)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)
- **VLANs in MST Instance** – VLANs assigned this instance.
- **MST ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **VLAN ID** – VLAN to assign to this selected MST instance. (Range: 1-4093)

The other global attributes are described under "Displaying Global Settings," page 3-157. The attributes displayed by the CLI for individual interfaces are described under "Displaying Interface Settings," page 3-166

Web – Click Spanning Tree, MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.

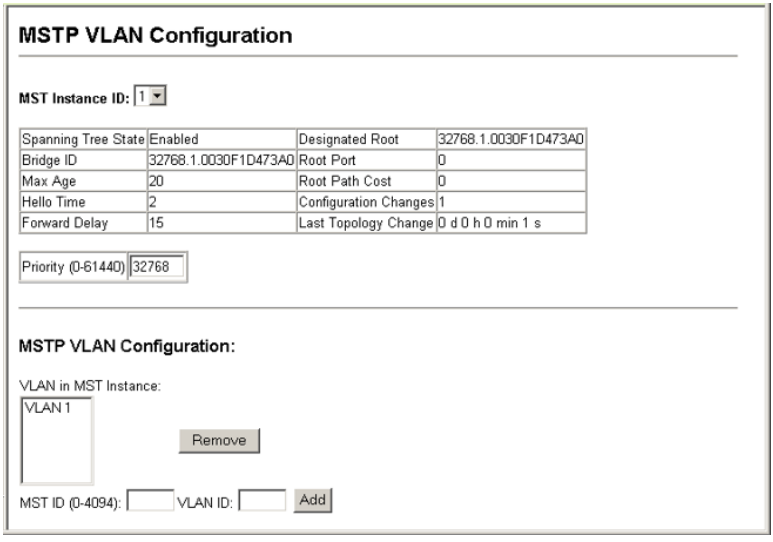


Figure 3-72 MSTP VLAN Configuration

CLI – This displays STA settings for instance 1, followed by settings for each port.

```
Console#show spanning-tree mst 1                                    4-243
Spanning-tree information
----------------------------------------------------------------
 Spanning tree mode:               MSTP
 Spanning tree enabled/disabled:   enabled
 Instance:                         1
 VLANs configuration:              1
 Priority:                         32768
 Bridge Hello Time (sec.):         2
 Bridge Max Age (sec.):            20
 Bridge Forward Delay (sec.):      15
 Root Hello Time (sec.):           2
 Root Max Age (sec.):              20
 Root Forward Delay (sec.):        15
 Max hops:                         20
 Remaining hops:                   20
 Designated Root:                  32768.1.0030F1D473A0
 Current root port:                7
 Current root cost:                10000
 Number of topology changes:       2
 Last topology changes time (sec.):85
 Transmission limit:               3
 Path Cost Method:                 long

----------------------------------------------------------------
Eth  1/ 7 information
----------------------------------------------------------------
 Admin status:                     enabled
 Role:                             master
 State:                            forwarding
 External admin path cost:         10000
 Internal admin path cost:         10000
 External oper path cost:          10000
 Internal oper path cost:          10000
 Priority:                         128
 Designated cost:                  0
 Designated port:                  128.1
 Designated root:                  32768.1.0030F1D473A0
 Designated bridge:                32768.1.0030F1D473A0
 Fast forwarding:                  disabled
 Forward transitions:              1
 Admin edge port:                  disabled
 Oper edge port:                   disabled
 Admin Link type:                  auto
 Oper Link type:                   point-to-point
 Spanning Tree Status:             enabled
:
```

CLI – This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

```
Console(config)#spanning-tree mst-configuration                    4-229
Console(config-mst)#mst 1 priority 4096                            4-231
Console(config-mstp)#mst 1 vlan 1-5                                4-230
Console(config-mst)#
```

Displaying Interface Settings for MSTP

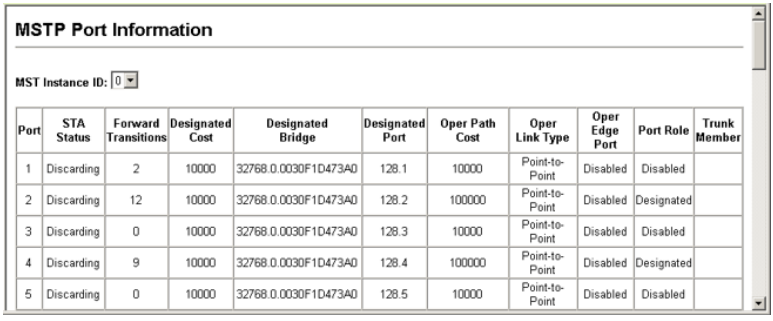
The MSTP Port Information and MSTP Trunk Information pages display the current status of ports and trunks in the selected MST instance.

Field Attributes

MST Instance ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

The other attributes are described under "Displaying Interface Settings," page 3-166.

Web – Click Spanning Tree, MSTP, Port Information or Trunk Information. Select the required MST instance to display the current spanning tree values.



MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Discarding	2	10000	32768.0.0030F1D473A0	128.1	10000	Point-to-Point	Disabled	Disabled	
2	Discarding	12	10000	32768.0.0030F1D473A0	128.2	100000	Point-to-Point	Disabled	Designated	
3	Discarding	0	10000	32768.0.0030F1D473A0	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Discarding	9	10000	32768.0.0030F1D473A0	128.4	100000	Point-to-Point	Disabled	Designated	
5	Discarding	0	10000	32768.0.0030F1D473A0	128.5	10000	Point-to-Point	Disabled	Disabled	

Figure 3-73 MSTP Port Information

CLI – This displays STA settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the IST (page 3-157), the settings for other instances only apply to the local spanning tree.

```
Console#show spanning-tree mst 0                                    4-243
Spanning-tree information
----------------------------------------------------------------------
 Spanning tree mode:               MSTP
 Spanning tree enabled/disabled:   enabled
 Instance:                         0
 VLANs configuration:              2-4093
 Priority:                         32768
 Bridge Hello Time (sec.):         2
 Bridge Max Age (sec.):            20
 Bridge Forward Delay (sec.):      15
 Root Hello Time (sec.):           2
 Root Max Age (sec.):              20
 Root Forward Delay (sec.):        15
 Max hops:                         20
 Remaining hops:                   20
 Designated Root:                  32768.0.0000E8AAAA00
 Current root port:                1
 Current root cost:                10000
 Number of topology changes:       12
 Last topology changes time (sec.):303
 Transmission limit:               3
 Path Cost Method:                 long

----------------------------------------------------------------------
Eth  1/ 1 information
----------------------------------------------------------------------
 Admin status:                     enabled
 Role:                             root
 State:                            forwarding
 External admin path cost:         10000
 Internal admin path cost:         10000
 External oper path cost:          10000
 Internal oper path cost:          10000
 Priority:                         128
 Designated cost:                  0
 Designated port:                  128.4
 Designated root:                  32768.0.0000E8AAAA00
 Designated bridge:                32768.0.0000E8AAAA00
 Fast forwarding:                  disabled
 Forward transitions:              2
 Admin edge port:                  disabled
 Oper edge port:                   disabled
 Admin Link type:                  auto
 Oper Link type:                   point-to-point
 Spanning Tree Status:             enabled
:
```

Configuring Interface Settings for MSTP

You can configure the STA interface settings for an MST Instance using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 3-166 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16

- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-161), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

  - Range –
    - Ethernet: 200,000-20,000,000
    - Fast Ethernet: 20,000-2,000,000
    - Gigabit Ethernet: 2,000-200,000
    - 10 Gigabit Ethernet: 200-20,000
  - Default –
    - Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
    - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
    - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000
    - 10 Gigabit Ethernet – Full duplex: 1000; trunk: 500

Web – Click Spanning Tree, MSTP, Port or Trunk Configuration. Enter the priority and path cost for an interface, and click Apply.

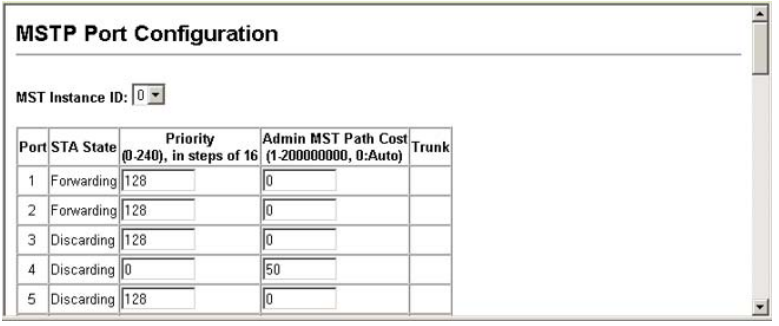


Figure 3-74 MSTP Port Configuration

CLI – This example sets the MSTP attributes for port 4.

```
Console(config)#interface ethernet 1/4                          4-187
Console(config-if)#spanning-tree mst port-priority 0            4-241
Console(config-if)#spanning-tree mst cost 50                    4-240
Console(config-if)
```

VLAN Configuration

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

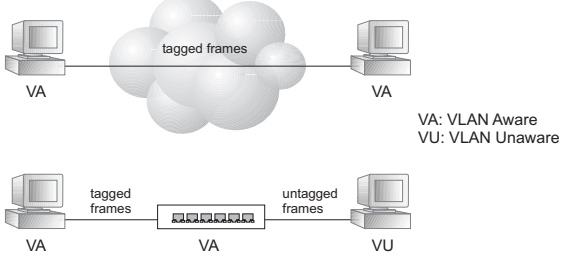
This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

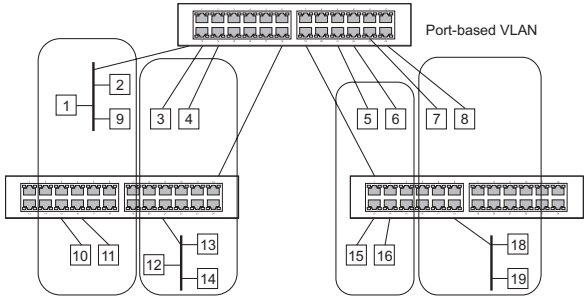
Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs (VLAN Index)" on page 3-190). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any

VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.
(Default: Disabled)

Web – Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, click Apply

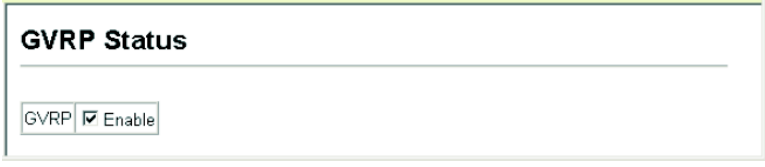


Figure 3-75 Globally Enabling GVRP

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp                                    4-264
Console(config)#
```

Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

- **VLAN Version Number**[15] – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

Web – Click VLAN, 802.1Q VLAN, Basic Information.

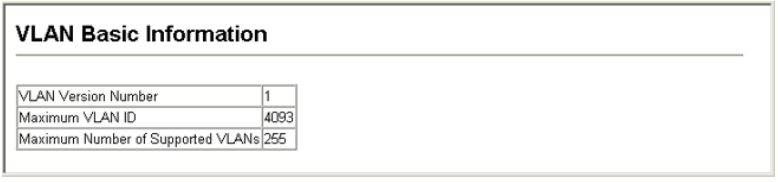


Figure 3-76 VLAN Basic Information

CLI – Enter the following command.

```
Console#show bridge-ext                                    4-265
 Max support VLAN numbers:              256
 Max support VLAN ID:                   4093
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Disabled
 GMRP:                                  Disabled
Console#
```

15. Web Only.

Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4093).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.

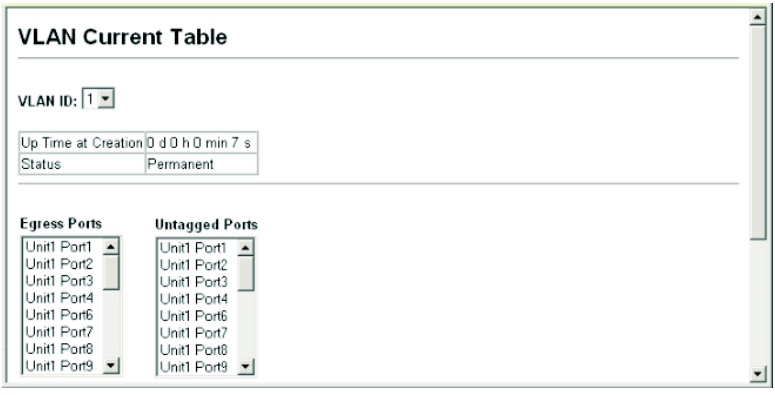


Figure 3-77 VLAN Current Table

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4093, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                          4-256

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S)
Console#
```

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4093).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status** (Web) – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **State** (CLI) – Enables or disables the specified VLAN.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

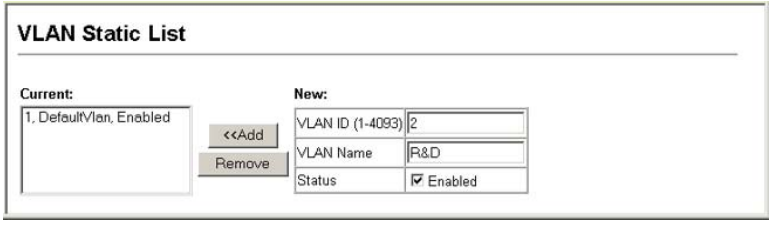


Figure 3-78 VLAN Static List - Creating VLANs

CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                          4-246
Console(config-vlan)#vlan 2 name R&D media ethernet state active       4-247
Console(config-vlan)#end
Console#show vlan                                                      4-256

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S)
.
.
.
VLAN ID:               2
Type:                  Static
Name:                  R&D
Status:                Active
Ports/Port Channels:

Console#
```

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

Notes: 1. You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 3-193). However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under "Configuring VLAN Behavior for Interfaces" on page 3-194.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4093).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see "Automatic VLAN Registration" on page 3-183.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.

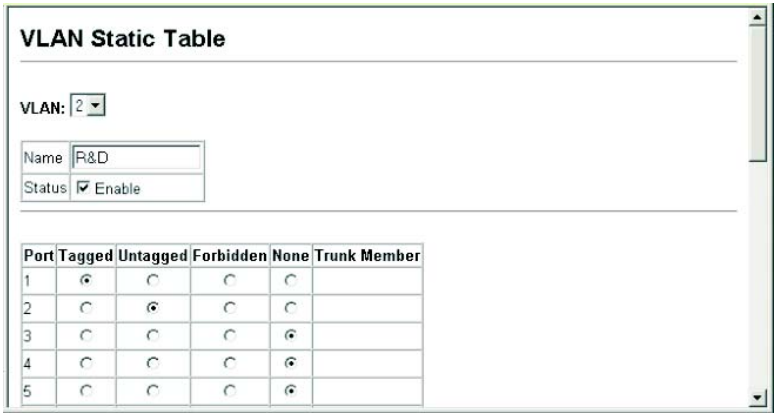


Figure 3-79 VLAN Static Table - Adding Static Members

CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                          4-187
Console(config-if)#switchport allowed vlan add 2 tagged         4-254
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#
```

Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, 802.1Q VLAN, Static Membership by Port. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.

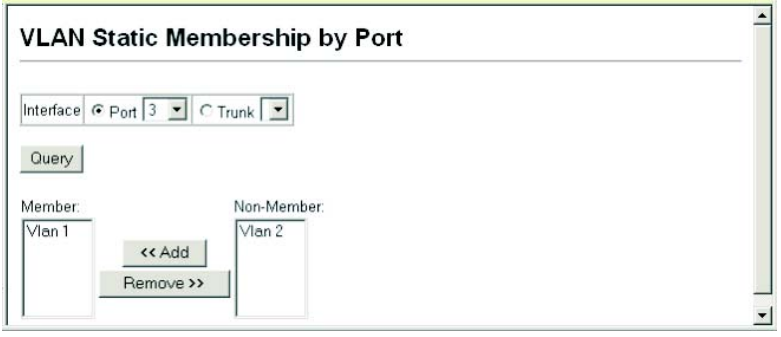


Figure 3-80 VLAN Static Membership by Port

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                          4-187
Console(config-if)#switchport allowed vlan add 1 tagged         4-254
Console(config-if)#switchport allowed vlan remove 2
Console(config-if)#
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/ deregistration.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to

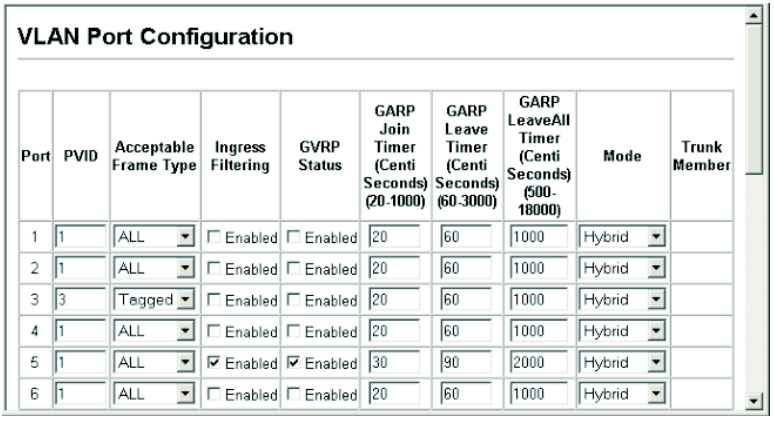
all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See "Displaying Bridge Extension Capabilities" on page 3-19.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)
- **GARP Join Timer**[16] – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave Timer** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)
- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

16. Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

- **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

• **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration. Fill in the required settings for each interface, click Apply.



VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
2	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
3	3	Tagged	Enabled	Enabled	20	60	1000	Hybrid	
4	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
5	1	ALL	Enabled	Enabled	30	90	2000	Hybrid	
6	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	

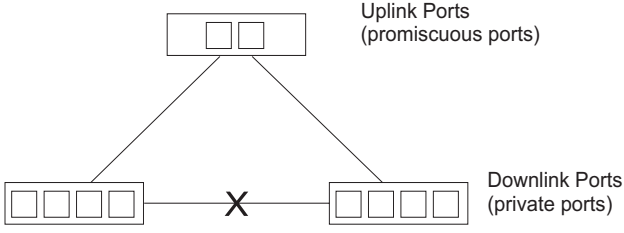
Figure 3-81 VLAN Port Configuration

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3                          4-187
Console(config-if)#switchport acceptable-frame-types tagged     4-251
Console(config-if)#switchport ingress-filtering                 4-252
Console(config-if)#switchport native vlan 3                     4-253
Console(config-if)#switchport gvrp                              4-266
Console(config-if)#garp timer join 20                           4-267
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid                       4-250
Console(config-if)#
```

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click VLAN, Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.

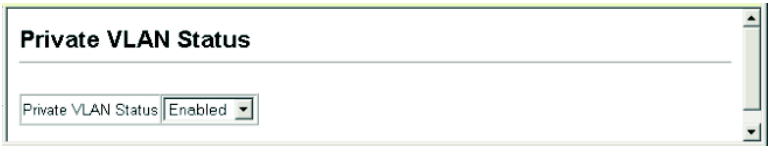


Figure 3-82 Private VLAN Status

CLI – This example enables private VLANs.

```
Console(config)#pvlan                                    4-257
Console(config)#
```

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Web – Click VLAN, Private VLAN, Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.



Figure 3-83 Private VLAN Link Status

CLI – This configures port 3 as an uplink and port 5 and 6 as downlinks.

```
Console(config)#pvlan up-link ethernet 1/3 down-link
  ethernet 1/5                                                  4-257
Console(config)#pvlan up-link ethernet 1/3 down-link
  ethernet 1/6
Console(config)#end
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/3
Down-link port:
 Ethernet 1/5
 Ethernet 1/6
Console#
```

Configuring Protocol-Based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 3-188). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.
3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

Configuring Protocol Groups

Create a protocol group for one or more protocols.

Command Attributes

- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **Frame Type**[17] – Frame type used by this protocol. (Options: Ethernet, RFC_1042, LLC_other)
- **Protocol Type** – The only option for the LLC_other frame type is IPX_raw. The options for all other frames types include: IP, ARP, RARP.

Web – Click VLAN, Protocol VLAN, Configuration. Enter a protocol group ID, frame type and protocol type, then click Apply.

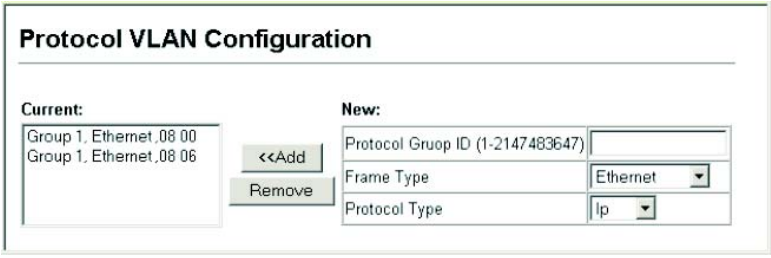


Figure 3-84 Protocol VLAN Configuration

CLI – The following creates protocol group 1, and then specifies Ethernet frames with IP and ARP protocol types.

```
Console(config)#protocol-vlan protocol-group 1
  add frame-type ethernet protocol-type ip                    4-260
Console(config)#protocol-vlan protocol-group 1
  add frame-type ethernet protocol-type arp
Console(config)#
```

17. SNAP frame types are not supported by this switch due to hardware limitations.

Mapping Protocols to VLANs

Map a protocol group to a VLAN for each interface that will participate in the group.

Command Usage

- When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN menus such as the VLAN Static Table (page 3-190) or VLAN Static Membership by Port menu (page 3-193), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

Web – Click VLAN, Protocol VLAN, Port Configuration. Select a a port or trunk, enter a protocol group ID, the corresponding VLAN ID, and click Apply.

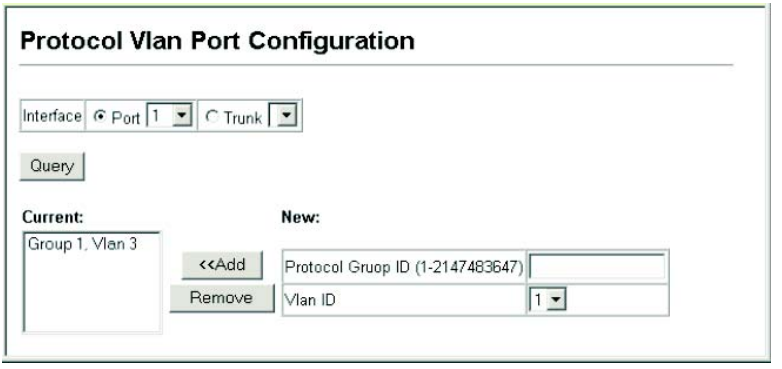


Figure 3-85 Protocol VLAN Port Configuration

CLI – The following maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 3.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 3      4-261
Console(config-if)#
```

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Layer 2 Queue Settings

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority**[18] – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)

18. CLI displays this information as "Priority for untagged traffic."

- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.

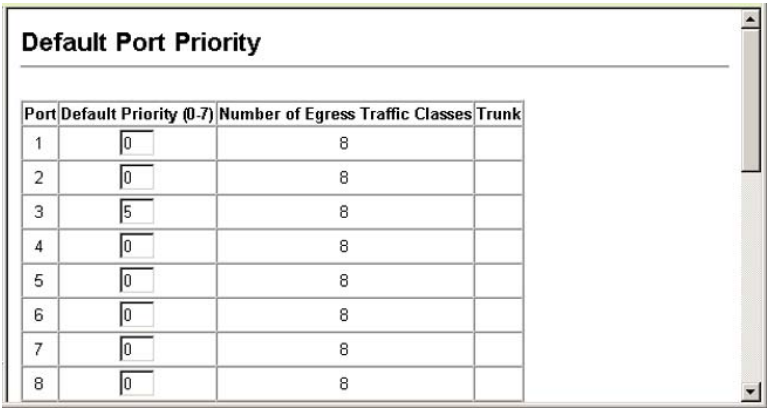


Figure 3-86 Default Port Priority

CLI – This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3                          4-187
Console(config-if)#switchport priority default 5                4-271
Console(config-if)#end
Console#show interfaces switchport ethernet 1/5                 4-199
Information of Eth 1/5
 Broadcast threshold:           Enabled, 500 packets/second
 LACP status:                   Disabled
 Ingress rate limit:            Disable, 1000M bits per second
 Egress rate limit:             Disable, 1000M bits per second
 VLAN membership mode:          Hybrid
 Ingress rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 GVRP status:                   Disabled
 Allowed VLAN:                     1(u),
 Forbidden VLAN:
Console#
```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 3-12 Mapping CoS Values to Egress Queues

Queue	0	1	2	3	4	5	6	7
Priority	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Table 3-13 CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class**[19] – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

19. CLI shows Queue ID.

Web – Click Priority, Traffic Classes. Assign priorities to the traffic classes (i.e., output queues), then click Apply.

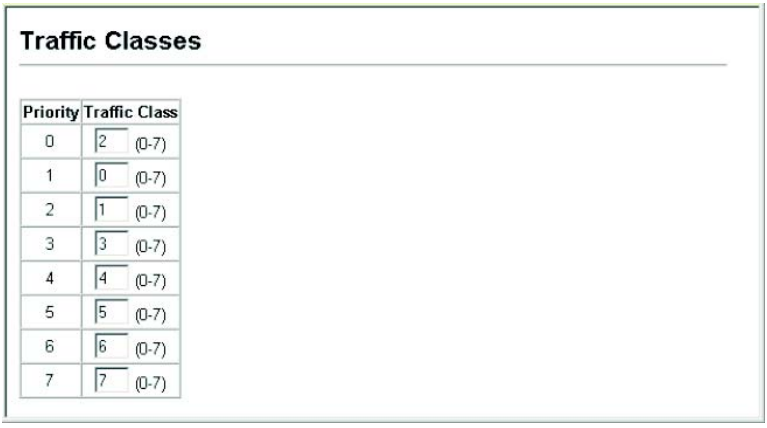


Figure 3-87 Traffic Classes

CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1                          4-187
Console(config)#queue cos-map 0 0                               4-273
Console(config)#queue cos-map 1 1
Console(config)#queue cos-map 2 2
Console(config)#exit
Console#show queue cos-map                                      4-275
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Information of Eth 1/2
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
:
```

* Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes

- **WRR** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively. (This is the default selection.)
- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Web – Click Priority, Queue Mode. Select Strict or WRR, then click Apply.

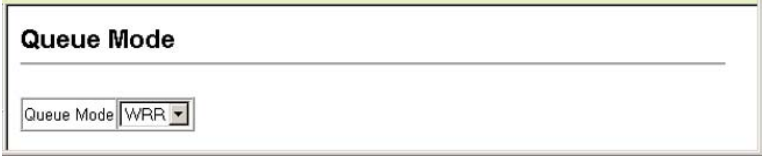


Figure 3-88 Queue Mode

CLI – The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict                                    4-274
Console(config)#exit
Console#show queue mode                                              4-274

Queue mode: strict
Console#
```

Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in "Mapping CoS Values to Egress Queues" on page 3-205, the traffic classes are mapped to one of the eight egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table**[20] – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Set a new weight for the selected traffic class. (Range: 1-15)

Web – Click Priority, Queue Scheduling. Select the interface, highlight a traffic class (i.e., output queue), enter a weight, then click Apply.

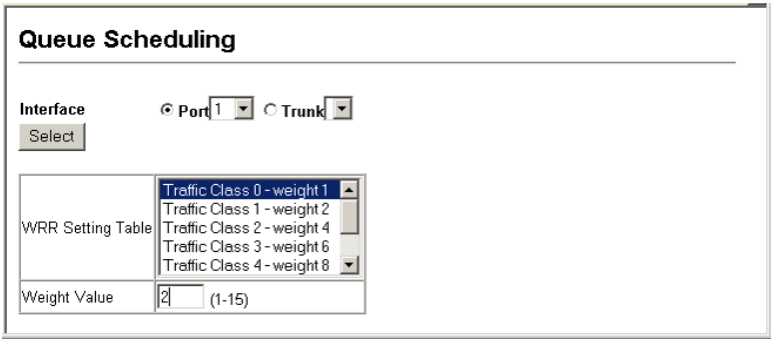


Figure 3-89 Queue Scheduling

20. CLI shows Queue ID.

CLI – The following example shows how to assign WRR weights to each of the priority queues.

```
Console(config)#queue bandwidth 1 3 5 7 9 11 13 15            4-272
Console(config)#exit
Console#show queue bandwidth                                  4-275
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0         1
    1         3
    2         5
    3         7
    4         9
    5         11
    6         13
    7         15
Information of Eth 1/2
 Queue ID  Weight
⋮
```

Layer 3/4 Priority Settings

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu, then click Apply.



Figure 3-90 IP Precedence/DSCP Priority Status

CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                              4-278
Console(config)#
```

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Table 3-14 Mapping IP Precedence

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precedence value. Note that "0" represents low priority and "7" represent high priority.

Web – Click Priority, IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.

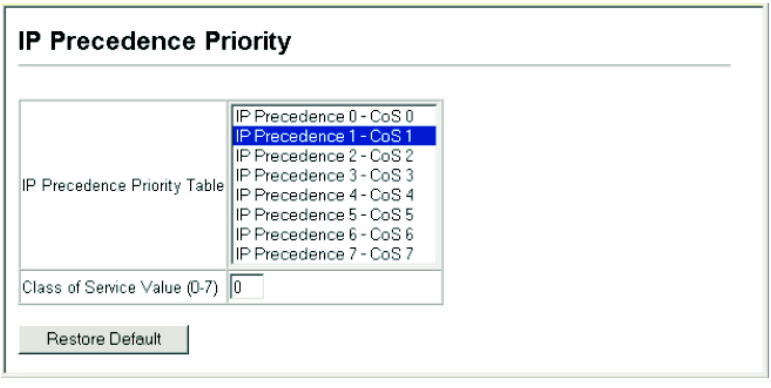

IP Precedence Priority
IP Precedence Priority Table
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7
Class of Service Value (0-7)
0
Restore Default

Figure 3-91 IP Precedence Priority

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```
Console(config)#map ip precedence                                4-278
Console(config)#interface ethernet 1/1                           4-187
Console(config-if)#map ip precedence 1 cos 0                     4-278
Console(config-if)#end
Console#show map ip precedence ethernet 1/1                      4-282
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 3-15 Mapping DSCP Priority

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that "0" represents low priority and "7" represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.

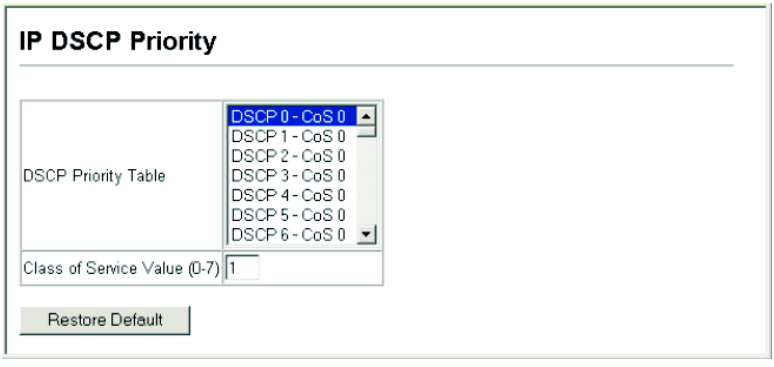

IP DSCP Priority
DSCP Priority Table
DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
Class of Service Value (0-7)
1
Restore Default

Figure 3-92 IP DSCP Priority

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp                                    4-279
Console(config)#interface ethernet 1/1                         4-187
Console(config-if)#map ip dscp 1 cos 0                         4-280
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                          4-283
DSCP mapping status: disabled

 Port       DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
:
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Port Priority

You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that "0" represents low priority and "7" represent high priority.

Note: IP Port Priority settings apply to all interfaces.

Web – Click Priority, IP Port Status. Set IP Port Priority Status to Enabled.

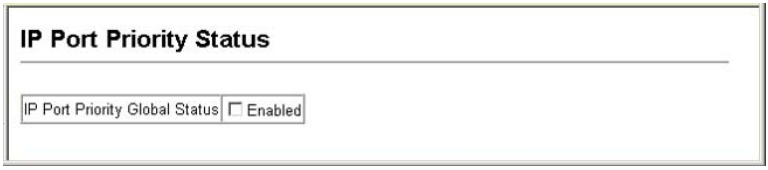


Figure 3-93 IP Port Priority Status

Click Priority, IP Port Priority. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Apply.

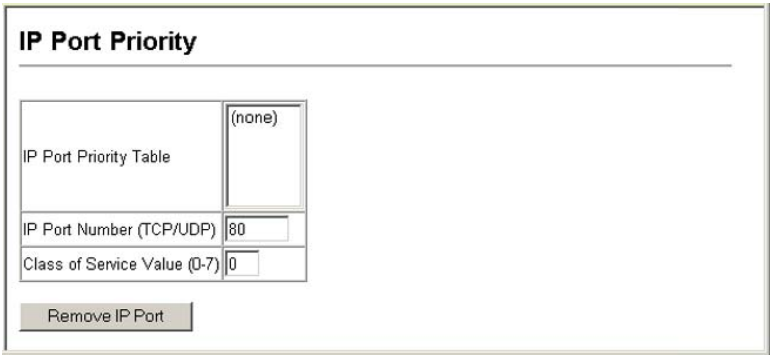


Figure 3-94 IP Port Priority

CLI – The following example globally enables IP Port Priority service on the switch, maps HTTP traffic (on port 1) to CoS value 0, and then displays the IP Port Priority settings.

```
Console(config)#map ip port                                    4-276
Console(config)#interface ethernet 1/1                         4-187
Console(config-if)#map ip port 80 cos 0                        4-277
Console(config-if)#end
Console#show map ip port ethernet 1/5                          4-281
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 1       80   0
Console#
```

* Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Quality of Service

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Notes: **1.** You can only configure one rule per Class Map. However, you can include multiple classes in a Policy Map.

2. You must create a Class Map before creating a Policy Map.

Configuring Quality of Service Parameters

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the "Class Map" to designate a class name for a specific category of traffic.
2. Edit the rules for each class to specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Set an ACL mask to enable filtering for the criteria specified in the Class Map. (See "Configuring an IP ACL Mask" on page 3-113 or "Configuring a MAC ACL Mask" on page 3-115.)
4. Use the "Policy Map" to designate a policy name for a specific manner in which ingress traffic will be handled.
5. Add one or more classes to the Policy Map. Assign policy rules to each class by "setting" the QoS value to be assigned to the matching traffic class. The policy rule can also be configured to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
6. Use the "Service Policy" to assign a policy map to a specific interface.

Configuring a Class Map

A class map is used for matching packets to a specified class.

Command Usage

- To configure a Class Map, follow these steps:
  - Open the Class Map page, and click Add Class.
  - When the Class Configuration page opens, fill in the "Class Name" field, and click Add.
  - When the Match Class Settings page opens, specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN, and click the Add button next to the field for the selected traffic criteria. You can only specify one item to match when assigning ingress traffic to a class map.
- The class map uses the Access Control List filtering engine, so you must also set an ACL mask to enable filtering for the criteria specified in the Class Map. See "Configuring an IP ACL Mask" on page 3-113 or "Configuring a MAC ACL Mask" on page 3-115 for information on configuring an appropriate ACL mask.
- The class map is used with a policy map (page 3-221) to create a service policy (page 3-225) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

Command Attributes

Class Map

- **Modify Name and Description** – Configures the name and a brief description of a class map. (Range: 1-32 characters for the name; 1-256 characters for the description)
- **Edit Rules** – Opens the "Match Class Settings" page for the selected class entry. Modify the criteria used to classify ingress traffic on this page.
- **Add Class** – Opens the "Class Configuration" page. Enter a class name and description on this page, and click Add to open the "Match Class Settings" page. Enter the criteria used to classify ingress traffic on this page.

- **Remove Class** – Removes the selected class.

Class Configuration

- **Class Name** – Name of the class map. (Range: 1-32 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **Description** – A brief description of a class map. (Range: 1-256 characters)
- **Add** – Adds the specified class.
- **Back** – Returns to previous page with making any changes.

Match Class Settings

- **Class Name** – List of class maps.
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN** – A VLAN. (Range:1-4093)
- **Add** – Adds the specified criteria to the class. Only one entry is permitted per class.
- **Remove** – Deletes the selected criteria from the class.

Web – Click QoS, DiffServ, then click Add Class to create a new class, or Edit Rules to change the rules of an existing class.

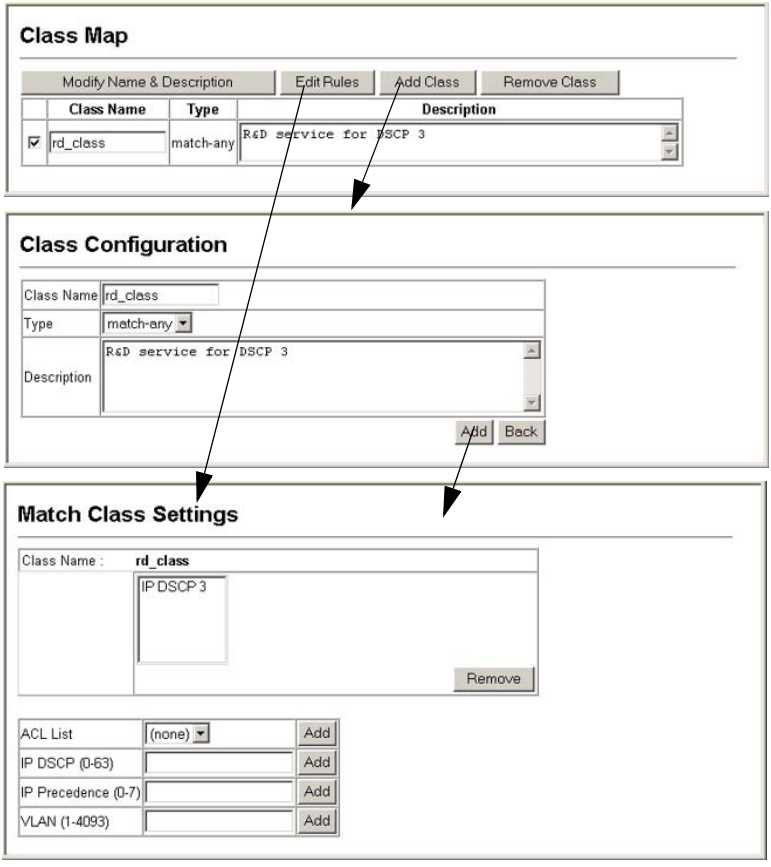


Figure 3-95 Configuring Class Maps

CLI - This example creates a class map call "rd-class," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd_class match-any                    4-286
Console(config-cmap)#match ip dscp 3                            4-287
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in               4-117
Console(config-ip-mask-acl)#mask any any dscp                   4-123
Console(config-ip-mask-acl)#
```

Creating QoS Policies

This function creates a policy map that can be attached to multiple interfaces.

Command Usage

- To configure a Policy Map, follow these steps:
  - Create a Class Map as described on page 3-218.
  - Open the Policy Map page, and click Add Policy.
  - When the Policy Configuration page opens, fill in the "Policy Name" field, and click Add.
  - When the Policy Rule Settings page opens, select a class name from the scroll-down list (Class Name field). Configure a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed field). Then finally click Add to register the new policy.
- A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings (page 3-225). You can configure up to 63 policers (i.e., class maps) for Fast Ethernet and Gigabit Ethernet ingress ports, and up to 225 policers for 10G Ethernet ingress ports.

  Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the "Burst" field, and the average rate tokens are removed from the bucket is by specified by the "Rate" option.

- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 3-225) to take effect.

Command Attributes

Policy Map

- **Modify Name and Description** – Configures the name and a brief description of a policy map. (Range: 1-32 characters for the name; 1-256 characters for the description)
- **Edit Classes** – Opens the "Policy Rule Settings" page for the selected class entry. Modify the criteria used to service ingress traffic on this page.
- **Add Policy** – Opens the "Policy Configuration" page. Enter a policy name and description on this page, and click Add to open the "Policy Rule Settings" page. Enter the criteria used to service ingress traffic on this page.
- **Remove Policy** – Deletes a specified policy.

Policy Configuration

- **Policy Name** — Name of policy map. (Range: 1-32 characters)
- **Description** – A brief description of a policy map. (Range: 1-256 characters)
- **Add** – Adds the specified policy.
- **Back** – Returns to previous page with making any changes.

Policy Rule Settings

- Class Settings -

- **Class Name** – Name of class map.
- **Action** – Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 3-218).
- **Meter** – The maximum throughput and burst rate.
  - **Rate (kbps)** – Rate in kilobits per second.
  - **Burst (byte)** – Burst in bytes.

- **Exceed Action** – Specifies whether the traffic that exceeds the specified rate will be dropped or the DSCP service level will be reduced.
- **Remove Class** – Deletes a class.

- Policy Options -

- **Class Name** – Name of class map.
- **Action** – Configures the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 3-218). (Range - CoS: 0-7, DSCP: 0-63, IP Precedence: 0-7)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
  - **Rate (kbps)** – Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
  - **Burst (byte)** – Burst in bytes. (Range: 64-1522)
- **Exceed** – Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.
  - **Set** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
  - **Drop** – Drops out of conformance traffic.
- **Add** – Adds the specified criteria to the policy map.

Web – Click QoS, DiffServ, Policy Map to display the list of existing policy maps. To add a new policy map click Add Policy. To configure the policy rule settings click Edit Classes.

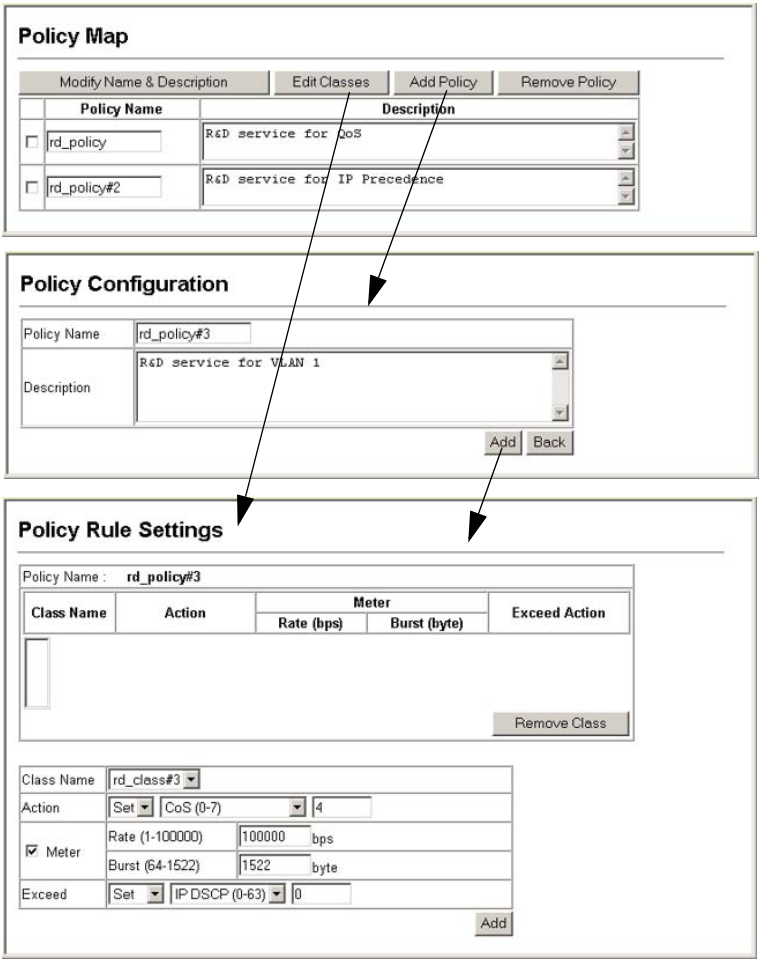


Figure 3-96 Configuring Policy Maps

CLI – This example creates a policy map called "rd-policy," sets the average bandwidth the 1 Mbps, the burst rate to 1522 bps, and the response to reduce the DSCP value for violating packets to 0.

```
Console(config)#policy-map rd_policy#3                          4-289
Console(config-pmap)#class rd_class#3                           4-290
Console(config-pmap-c)#set ip dscp 4                            4-291
Console(config-pmap-c)#police 100000 1522 exceed-action
  set ip dscp 0                                                 4-292
Console(config-pmap-c)#
```

Attaching a Policy Map to Ingress Queues

This function binds a policy map to the ingress queue of a particular interface.

Command Usage

- You must first define a class map, set an ACL mask to match the criteria defined in the class map, then define a policy map, and finally bind the service policy to the required interface.
- You can only bind one policy map to an interface.
- The current firmware does not allow you to bind a policy map to an egress queue.

Command Attributes

- **Ports** – Specifies a port.
- **Ingress** – Applies the rule to ingress traffic.
- **Enabled** – Check this to enable a policy map on the specified port.
- Policy Map – Select the appropriate policy map from the scroll-down box.

Web – Click QoS, DiffServ, Service Policy Settings. Check Enabled and choose a Policy Map for a port from the scroll-down box, then click Apply.

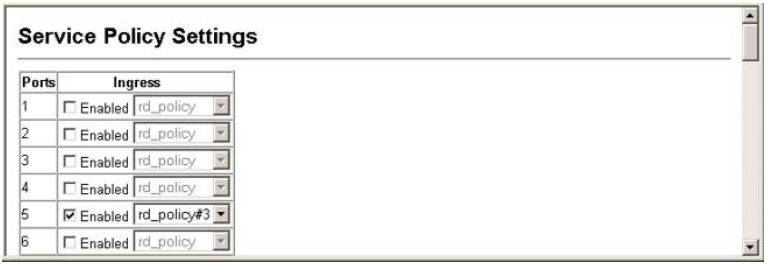


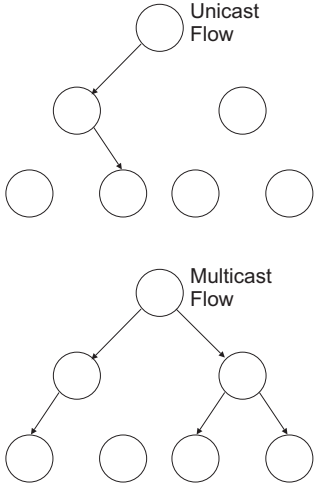
Figure 3-97 Service Policy Settings

CLI - This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/5                    4-187
Console(config-if)#service-policy input rd_policy#3       4-293
Console(config-if)#
```

Multicast Filtering

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully



pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 3-228) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 3-231). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 3-233).

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)
- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-25 seconds, Default: 10)
- **IGMP Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Range: 1-2; Default: 2)

Notes: **1.** All systems on the subnet must support the same version.
2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)

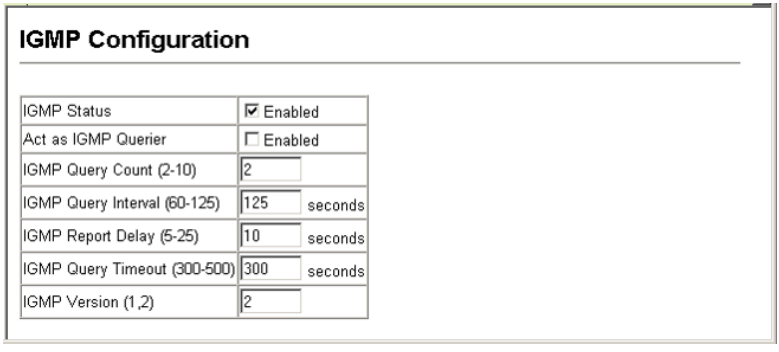


Figure 3-98 IGMP Configuration

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                                  4-297
Console(config)#ip igmp snooping querier                          4-301
Console(config)#ip igmp snooping query-count 10                   4-301
Console(config)#ip igmp snooping query-interval 100               4-302
Console(config)#ip igmp snooping query-max-response-time 20       4-303
Console(config)#ip igmp snooping query-time-out 300               4-304
Console(config)#ip igmp snooping version 2                        4-298
Console(config)#exit
Console#show ip igmp snooping                                     4-299
 Service status:           Enabled
 Querier status:           Enabled
 Query count:              10
 Query interval:           100 sec
 Query max response time:  20 sec
 Router port expire time:  300 sec
 IGMP snooping version:    Version 2
Console#
```

Displaying Interfaces Attached to a Multicast Router

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4093).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.

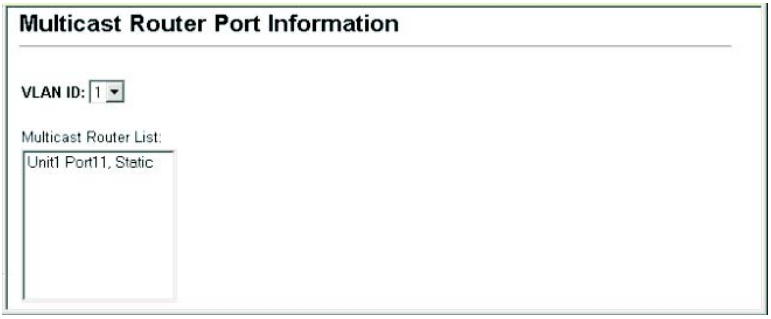


Figure 3-99 Multicast Router Port Information

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                    4-306
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
Console#
```

Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.

- **Unit** – Stack unit. (Range: 1-8)
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.

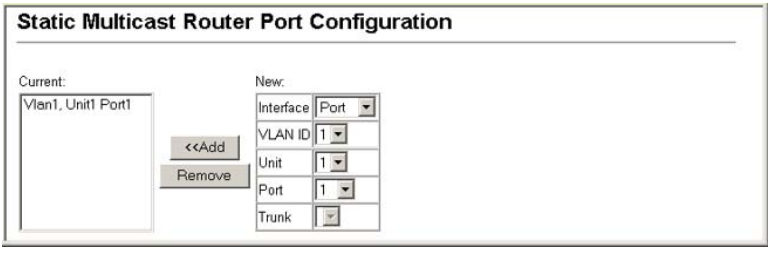


Figure 3-100 Static Multicast Router Port Configuration

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11 4-305
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                  4-306
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11  Static
Console#
```

Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.



Figure 3-101 IP Multicast Registration Table

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

```
Console#show mac-address-table multicast vlan 1                4-299
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12       Eth1/12    USER
    1       224.1.2.3       Eth1/12    IGMP
Console#
```

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in "Configuring IGMP Snooping and Query Parameters" on page 3-228. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Unit** – Stack unit. (Range: 1-8)
- **Port** or **Trunk** – Specifies the interface attached to a multicast router/switch.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.

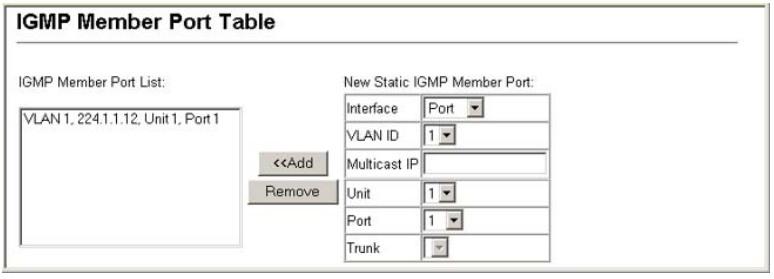


Figure 3-102 IGMP Member Port Table

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
 ethernet 1/12                                              4-297
Console(config)#exit
Console#show mac-address-table multicast vlan 1             4-299
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
```

Configuring Domain Name Service

The Domain Naming System (DNS) service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Configuring General DNS Server Parameters

Command Usage

- To enable DNS service on this switch, first configure one or more name servers, and then enable domain lookup status.
- To append domain names to incomplete host names received from a DNS client (i.e., not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.
- If there is no domain list, the default domain name is used. If there is a domain list, the default domain name is not used.

- When an incomplete host name is received by the DNS server on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- Note that if all name servers are deleted, DNS will automatically be disabled.

Command Attributes

- **Domain Lookup Status** – Enables DNS host name-to-address translation.
- **Default Domain Name**[21] – Defines the default domain name appended to incomplete host names. (Range: 1-64 alphanumeric characters)
- **Domain Name List** – Defines a list of domain names that can be appended to incomplete host names. (Range: 1-64 alphanumeric characters. 1-5 names)
- **Name Server List** – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

21. Do not include the initial dot that separates the host name from the domain name.

Web – Select DNS, General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use to use for address resolution, enable domain lookup status, and click Apply.

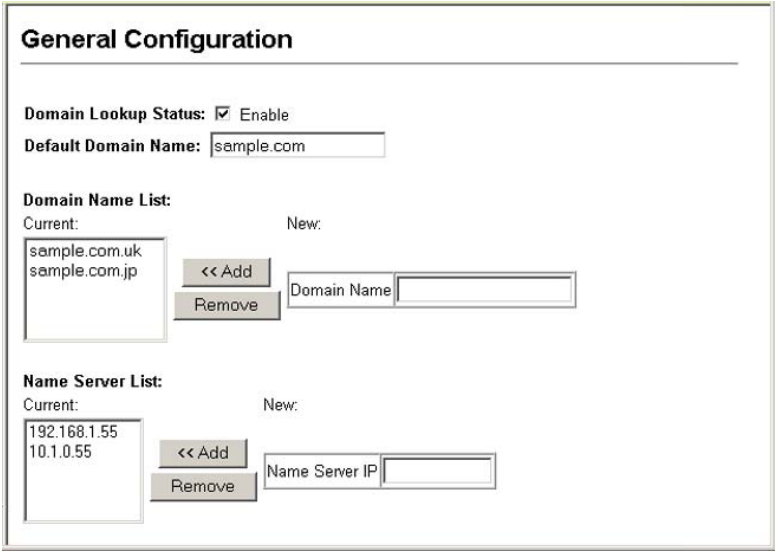


Figure 3-103 DNS General Configuration

CLI - This example sets a default domain name and a domain list. However, remember that if a domain list is specified, the default domain name is not used.

```
Console(config)#ip domain-name sample.com                    4-179
Console(config)#ip domain-list sample.com.uk                 4-180
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-server 192.168.1.55 10.1.0.55      4-181
Console(config)#ip domain-lookup                             4-182
Console#show dns                                             4-184
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.uk
    .sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Configuring Static DNS Host to Address Entries

You can manually configure static entries in the DNS table that are used to map domain names to IP addresses.

Command Usage

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.
- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Field Attributes

- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-64 characters)
- **IP Address** – Internet address(es) associated with a host name. (Range: 1-8 addresses)
- **Alias** – Displays the host names that are mapped to the same address(es) as a previously configured entry.

Web – Select DNS, Static Host Table. Enter a host name and one or more corresponding addresses, then click Apply.

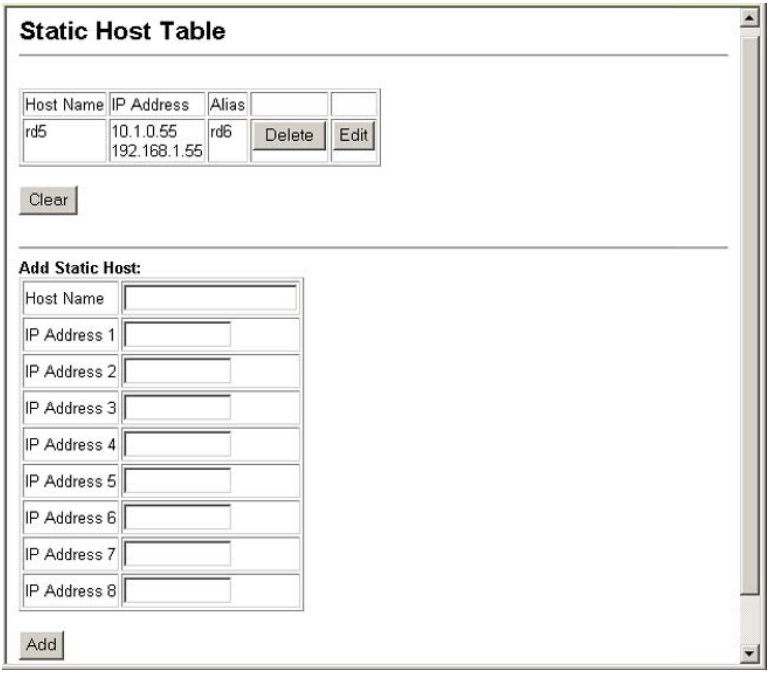


Figure 3-104 DNS Static Host Table

CLI - This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55            4-178
Console(config)#ip host rd6 10.1.0.55
Console#show host                                             4-183

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```

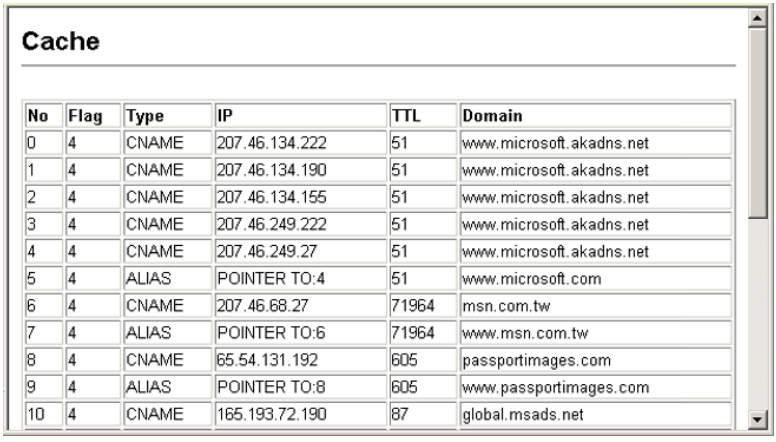
Displaying the DNS Cache

You can display entries in the DNS cache that have been learned via the designated name servers.

Field Attributes

- **No** – The entry number for each resource record.
- **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

Web – Select DNS, Cache.



Cache

No	Flag	Type	IP	TTL	Domain
0	4	CNAME	207.46.134.222	51	www.microsoft.akadns.net
1	4	CNAME	207.46.134.190	51	www.microsoft.akadns.net
2	4	CNAME	207.46.134.155	51	www.microsoft.akadns.net
3	4	CNAME	207.46.249.222	51	www.microsoft.akadns.net
4	4	CNAME	207.46.249.27	51	www.microsoft.akadns.net
5	4	ALIAS	POINTER TO:4	51	www.microsoft.com
6	4	CNAME	207.46.68.27	71964	msn.com.tw
7	4	ALIAS	POINTER TO:6	71964	www.msn.com.tw
8	4	CNAME	65.54.131.192	605	passportimages.com
9	4	ALIAS	POINTER TO:8	605	www.passportimages.com
10	4	CNAME	165.193.72.190	87	global.msads.net

Figure 3-105 DNS Cache

CLI - This example displays all the resource records learned from the designated name servers.

```
Console#show dns cache                                              4-184
NO       FLAG     TYPE     IP               TTL      DOMAIN
0          4      CNAME    207.46.134.222   51       www.microsoft.akadns.net
1          4      CNAME    207.46.134.190   51       www.microsoft.akadns.net
2          4      CNAME    207.46.134.155   51       www.microsoft.akadns.net
3          4      CNAME    207.46.249.222   51       www.microsoft.akadns.net
4          4      CNAME    207.46.249.27    51       www.microsoft.akadns.net
5          4      ALIAS    POINTER TO:4     51       www.microsoft.com
6          4      CNAME    207.46.68.27     71964    msn.com.tw
7          4      ALIAS    POINTER TO:6     71964    www.msn.com.tw
8          4      CNAME    65.54.131.192    605      passportimages.com
9          4      ALIAS    POINTER TO:8     605      www.passportimages.com
10         4      CNAME    165.193.72.190   87       global.msads.net
Console#
```

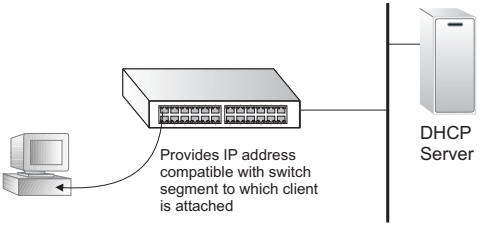
Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet.

When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

Configuring DHCP Relay Service

This switch supports DHCP relay service for attached host devices. If DHCP relay is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.



Command Usage

You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.

Command Attributes

- **VLAN ID** – ID of configured VLAN.
- **VLAN Name** – Name of the VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.
- **Restart DHCP Relay** – Use this button to enable or re-initialize DHCP relay service.

Web – Click DHCP, Relay Configuration. Enter up to five IP addresses for any VLAN, then click Restart DHCP Relay to start the relay service.

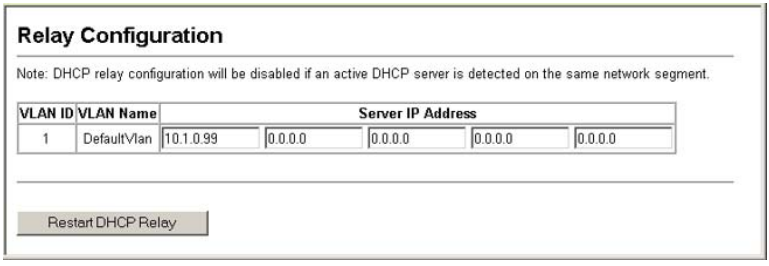


Figure 3-106 DHCP Relay Configuration

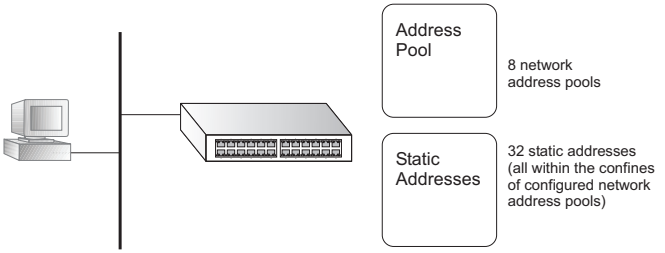
CLI – This example specifies one DHCP relay server for VLAN 1, and enables the relay service.

```
Console(config)#interface vlan 1                              4-187
Console(config-if)#dhcp relay server 10.1.0.99                4-160
Console(config-if)#ip dhcp relay                              4-159
Console(config-if)#
```

Configuring the DHCP Server

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.


Address Pool
8 network address pools
Static Addresses
32 static addresses (all within the confines of configured network address pools)

Command Usage

- First configure any excluded addresses, including the address for this switch.
- Then configure address pools for the network interfaces. You can configure up to 8 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. You can configure up to 32 fixed host addresses (i.e., entering one address per pool).
- If the DHCP server is running, you must disable it and then reenable it to implement any configuration changes. This can be done on the DHCP, Server, General page.

Enabling the Server, Setting Excluded Addresses

Enable the DHCP Server and specify the IP addresses that it should not be assigned to clients.

Command Attributes

- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)
- **Excluded Addresses** – Specifies IP addresses that the DHCP server should not assign to DHCP clients. You can specify a single address or an address range.
- **New** (Excluded Addresses) – New entries for excluded addresses can be specified as a single address or an address range.

Note: Be sure you exclude the address for this switch and other key network devices.

Web – Click DHCP, Server, General. Enter a single address or an address range, and click Add.

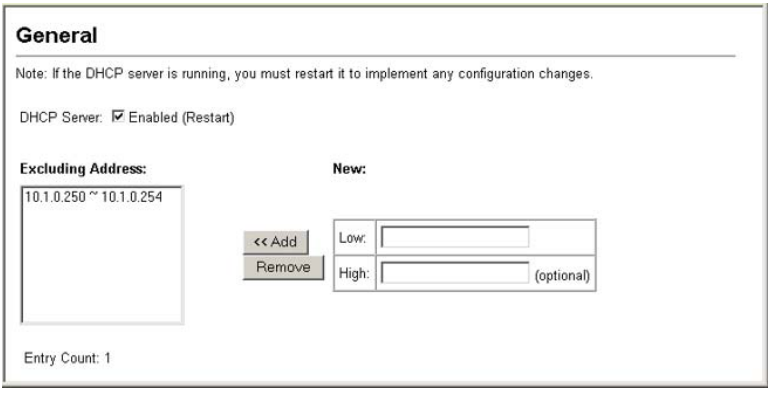


Figure 3-107 DHCP Server General Configuration

CLI – This example enables the DHCP and sets an excluded address range.

```
Console(config)#service dhcp                                    4-162
Console(config)#ip dhcp excluded-address 10.1.0.250
  10.1.0.254                                                    4-163
Console#
```

Configuring Address Pools

You must configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

Command Usage

- First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., one address per host pool).
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.

- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see page 3-295). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the IP Excluded Address field on the DHCP Server General configuration page.

Command Attributes

Creating a New Address Pool

Pool Name – A string or integer. (Range: 1-8 characters)

Setting the Network Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Setting the Host Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – Specifies the network mask of the client.
- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI; Default: Ethernet)
- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value.

Setting the Optional Parameters

- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.

- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-32 characters)
- **Bootfile** – The default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: fixed period, Infinite; Default: 1 day)

Examples

Creating a New Address Pool

Web – Click DHCP, Server, Pool Configuration. Specify a pool name, then click Add.

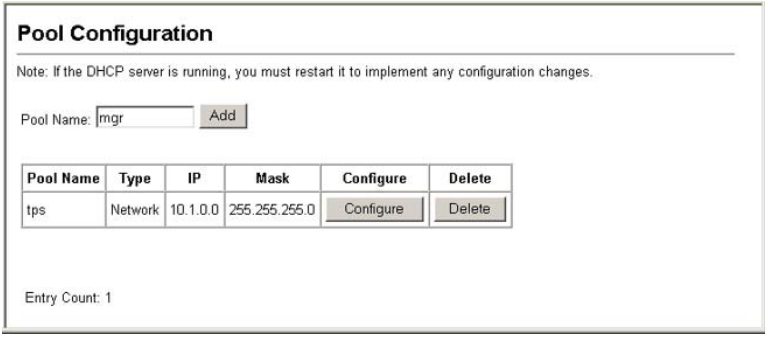


Figure 3-108 DHCP Server Pool Configuration

CLI – This example adds an address pool and enters DHCP pool configuration mode.

```
Console(config)#ip dhcp pool mgr                                    4-163
Console(config-dhcp)#
```

Configuring a Network Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for "Network." Enter the IP address and subnet mask for the network pool. Configure the optional parameters such as gateway server and DNS server. Then click Apply.

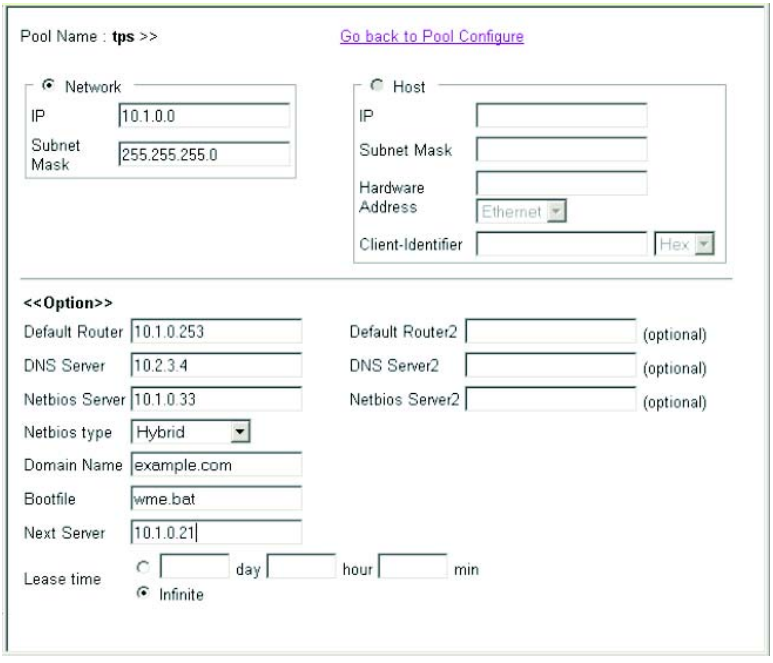


Figure 3-109 DHCP Server Pool - Network Configuration

CLI – This example configures a network address pool.

```
Console(config)#ip dhcp pool tps                                    4-163
Console(config-dhcp)#network 10.1.0.0 255.255.255.0                4-164
Console(config-dhcp)#default-router 10.1.0.253                      4-165
Console(config-dhcp)#dns-server 10.2.3.4                            4-167
Console(config-dhcp)#netbios-name-server 10.1.0.33                  4-169
Console(config-dhcp)#netbios-node-type hybrid                       4-170
Console(config-dhcp)#domain-name example.com                        4-166
Console(config-dhcp)#bootfile wme.bat                               4-168
Console(config-dhcp)#next-server 10.1.0.21                          4-167
Console(config-dhcp)#lease infinite                                 4-171
Console(config-dhcp)#
```

Configuring a Host Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for "Host." Enter the IP address, subnet mask, and hardware address for the client device. Configure the optional parameters such as gateway server and DNS server. Then click Apply.

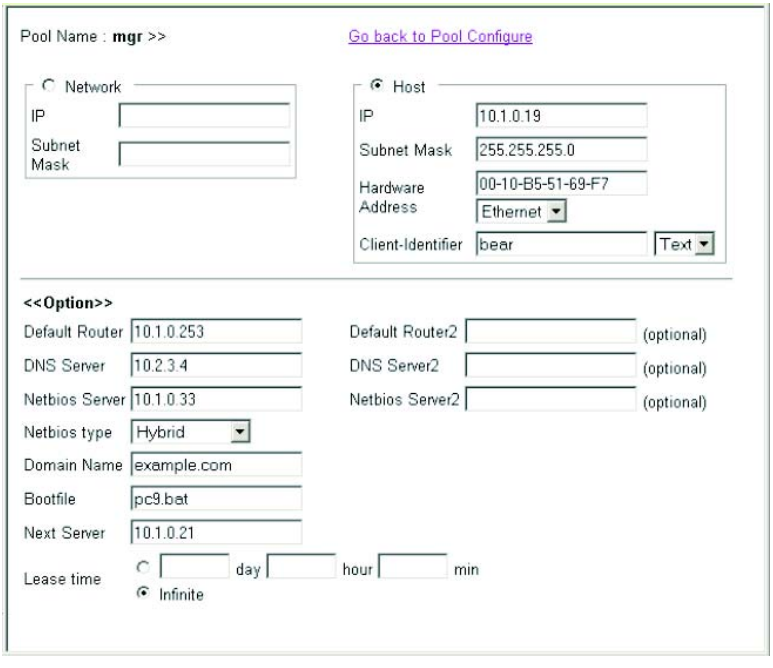


Figure 3-110 DHCP Server Pool - Host Configuration

CLI – This example configures a host address pool.

```
Console(config)#ip dhcp pool mgr                                    4-163
Console(config-dhcp)#host 10.1.0.19 255.255.255.0                   4-172
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28
  ethernet                                                          4-174
Console(config-dhcp)#client-identifier text bear                    4-173
Console(config-dhcp)#default-router 10.1.0.253                      4-165
Console(config-dhcp)#dns-server 10.2.3.4                            4-167
Console(config-dhcp)#netbios-name-server 10.1.0.33                  4-169
Console(config-dhcp)#netbios-node-type hybrid                       4-170
Console(config-dhcp)#domain-name example.com                        4-166
Console(config-dhcp)#bootfile wme.bat                               4-168
Console(config-dhcp)#next-server 10.1.0.21                          4-167
Console(config-dhcp)#lease infinite                                 4-171
Console(config-dhcp)#
```

Displaying Address Bindings

You can display the host devices which have acquired an IP address from this switch's DHCP server.

Command Attributes

- **IP Address** – IP address assigned to host.
- **Mac Address** – MAC address of host.
- **Lease time** – Duration that this IP address can be used by the host.
- **Start time** – Time this address was assigned by the switch.
- **Delete** – Clears this binding to the host. This command is normally used after modifying the address pool, or after moving DHCP service to another device.
- **Entry Count** – Number of hosts that have been given addresses by the switch.

Note: More than one DHCP server may respond to a service request by a host. In this case, the host generally accepts the first address assigned by any DHCP server.

Web – Click DHCP, Server, IP Binding. You may use the Delete button to clear an address from the DHCP server's database.

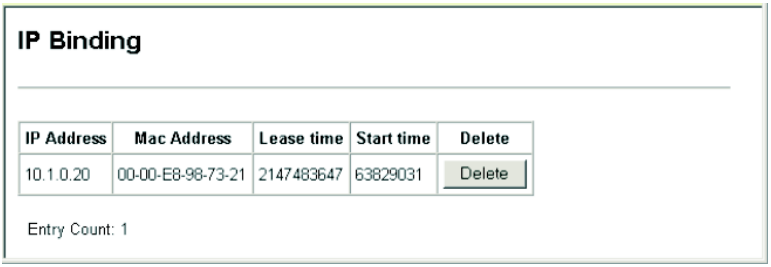


Figure 3-111 DHCP Server - IP Binding

CLI – This example displays the current binding, and then clears all automatic binding.

```
Console#show ip dhcp binding                                    4-176

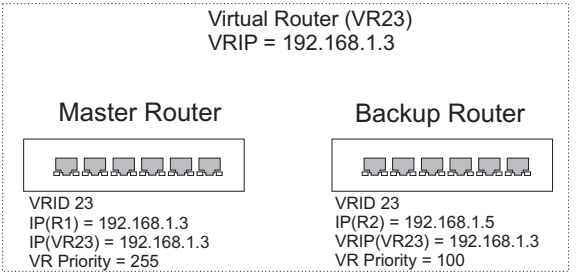
     IP                MAC          Lease Time     Start
--------------- ----------------- ------------ -----------
     10.1.0.20 00-00-e8-98-73-21         86400 Dec 25 08:01:57 2002
Console#clear ip dhcp binding *                                 4-175
Console#
```

Configuring Router Redundancy

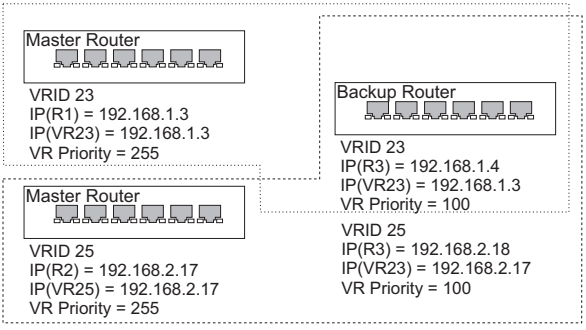
Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

This switch supports the Virtual Router Redundancy Protocol (VRRP). This protocol requires you to specify the interface of one of the routers participating in the virtual group as the address for the master virtual router. VRRP then selects the backup routers based on the specified virtual router priority. Router redundancy can be set up in any of the following configurations.

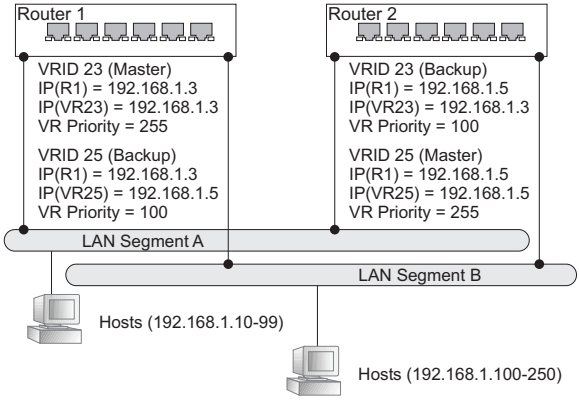
- A master virtual router with one or more backup routers.



- Several virtual master routers using the same set of backup routers.



- Several virtual master routers configured for mutual backup and load sharing. Load sharing can be accomplished by assigning a subset of addresses to different host address pools using the DHCP server. (See "Configuring Address Pools" on page 3-246.)



Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) allows you to configure a group of routers as a single virtual router. The virtual router group is configured with a single virtual IP address that can be used as the default gateway for host devices on the attached network.

Configuring VRRP Groups

To configure VRRP, select an interface on one router in the group to serve as the master virtual router. This physical interface is used as the virtual address for the router group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line.

Command Usage

Address Assignment –

- The IP address assigned to the virtual router must already be configured on the router that will be the Owner. In other words, the IP address for the virtual router exists on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.
- If you have multiple secondary addresses configured on the current VLAN interface, you can add any of these addresses to the virtual router group.
- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- VRRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

Virtual Router Priority –

- The Owner of the virtual IP address is automatically assigned the highest possible virtual router priority of 255. The backup router with the highest priority will become the master router if the current master fails. However, because the priority of the virtual IP address Owner is the highest, the original master router will always become the active master router when it recovers.
- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

Preempting the Acting Master –

- The virtual IP Owner has the highest priority, so no other router can preempt it, and it will always resume control as the master virtual router when it comes back on line. The preempt function only allows a backup router to take over from another backup router that is temporarily acting as the group master. If preemption is enabled and this router has a higher priority than the current acting master when it comes on line, it will take over as the acting group master.
- You can add a delay to the preempt function to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

Field Attributes (VRRP Group Configuration)

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4093; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **State** – VRRP router role. (Values: Master, Backup)
- **Virtual Address** – Virtual IP address for this group.
- **Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master.

- **Preemption** – Shows if this router is allowed to preempt the acting master.
- **Priority** – Priority of this router in the VRRP group.
- **AuthType** – Authentication mode used to verify VRRP packets from other routers.

Command Attributes (VRRP Group Configuration Detail)

- **Associated IP Table** – IP interfaces associated with this virtual router group.
- **Associated IP** – IP address of the virtual router, or secondary IP addresses assigned to the current VLAN interface that are supported by this VRRP group. If this address matches a real interface on this switch, then this interface will become the virtual master router for this VRRP group.
- **Advertisement Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master. (Range: 1-255 seconds; Default: 1 second)
  - VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
  - VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.
  - If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second.
- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router (i.e., another backup router that has taken over from the VRRP group address owner.) (Default: Enabled)
- **Preempt Delay** – Time to wait before issuing a claim to become the master. (Range: 0-120 seconds; 0 seconds)

- **Priority** – The priority of this router in a VRRP group. (Range: 1-254; Default: 100)
  - The priority for the VRRP group address owner is automatically set to 255.
  - The priority for backup routers is used to determine which router will take over as the acting master router if the current master fails.
- **Authentication Type** – Authentication mode used to verify VRRP packets received from other routers. (Options: None, Simple Text)
  - If simple text authentication is selected, then you must also enter an authentication string.
  - All routers in the same VRRP group must be set to the same authentication mode, and be configured with the same authentication string.
  - Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.
- **Authentication String** – Key used to authenticate VRRP packets received from other routers. (Range: 1-8 alphanumeric characters)
  - When a VRRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.

Web – Click IP, VRRP, Group Configuration. Select the VLAN ID, enter the VRID group number, and click Add.

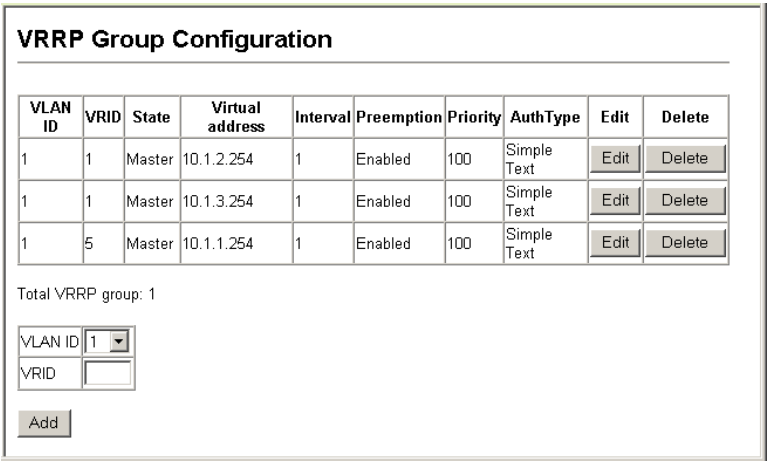


Figure 3-112 VRRP Group Configuration

Click the Edit button for a group entry to open the detailed configuration window. Enter the IP address of a real interface on this router to make it the master virtual router for the group. Otherwise, enter the virtual address for an existing group to make it a backup router. Click Add IP to enter an IP address into the Associated IP Table. Then set any of the other parameters as required, and click Apply.

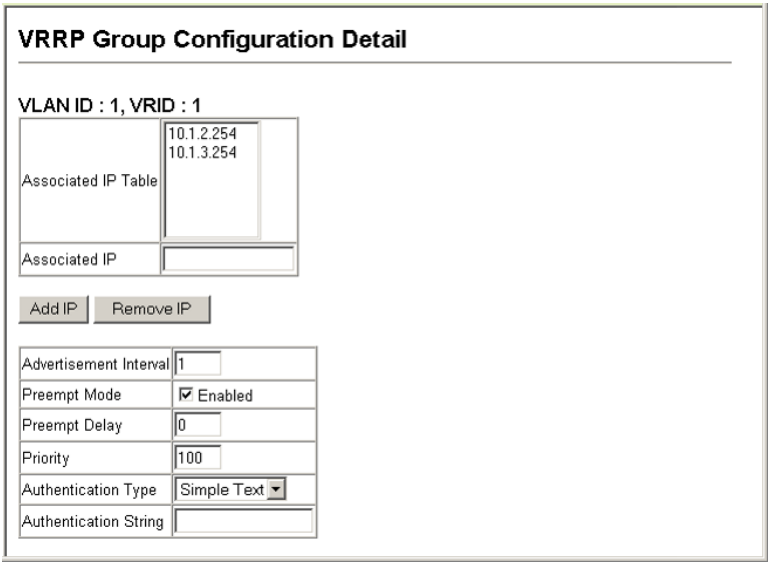


Figure 3-113 VRRP Group Configuration Detail

CLI – This example creates VRRP group 1, sets this switch as the master virtual router by assigning the primary interface address for the selected VLAN to the virtual IP address. It then adds a secondary IP address to the VRRP group, sets all of the other VRRP parameters, and then displays the configured settings.

```
Console(config)#interface vlan 1                                    4-249
Console(config-if)#vrrp 1 ip 192.168.1.6                            4-382
Console(config-if)#vrrp 1 ip 192.168.2.6 secondary
Console(config-if)#vrrp 1 timers advertise 5                        4-385
Console(config-if)#vrrp 1 preempt delay 10                          4-386
Console(config-if)#vrrp 1 priority 1                                4-384
Console(config-if)#vrrp 1 authentication bluebird                   4-383
Console(config-if)#end
Console#show vrrp                                                   4-387
 Vlan 1 - Group 1,
 state                          Master
 Virtual IP address             192.168.1.6
 Virtual MAC address            00-00-5E-00-01-01
 Advertisement interval         5 sec
 Preemption                     enabled
 Min delay                      10 sec
 Priority                       1
 Authentication                 SimpleText
 Authentication key             bluebird
 Master Router                  192.168.1.6
 Master priority                255
 Master Advertisement interval  5 sec
 Master down interval           15
Console#
```

Displaying VRRP Global Statistics

The VRRP Global Statistics page displays counters for errors found in VRRP protocol packets.

Field Attributes

- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number of VRRP packets received with an invalid VRID for this virtual router.

Web – Click IP, VRRP, Global Statistics.

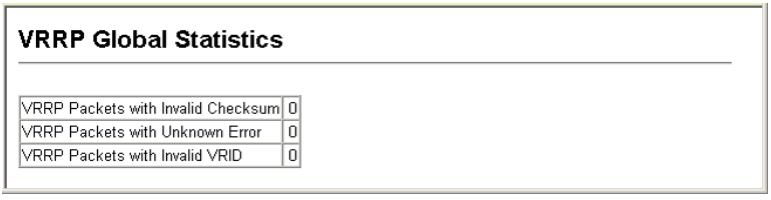

VRRP Global Statistics
VRRP Packets with Invalid Checksum 0
VRRP Packets with Unknown Error 0
VRRP Packets with Invalid VRID 0

Figure 3-114 VRRP Global Statistics

CLI – This example displays counters for protocol errors for all the VRRP groups configured on this switch.

```
Console#show vrrp router counters                                    4-390
  VRRP Packets with Invalid Checksum : 0
  VRRP Packets with Unknown Error    : 0
  VRRP Packets with Invalid VRID     : 0
Console#
```

Displaying VRRP Group Statistics

The VRRP Group Statistics page displays counters for VRRP protocol events and errors that have occurred on a specific VRRP interface.

Field Attributes

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4093; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **Times Become Master** – Number of times this router has transitioned to master.
- **Received Packets** – Number of VRRP advertisements received by this router.
- **Error Interval Packets** – Number of VRRP advertisements received for which the advertisement interval is different from the one configured for the local virtual router.
- **Authentication Failures** – Number of VRRP packets received that do not pass the authentication check.

- **Error IP TTL Packets** – Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
- **Received Priority 0 Packets** – Number of VRRP packets received by the virtual router with priority set to 0.
- **Error Packet Length Packets** – Number of packets received with a packet length less than the length of the VRRP header.
- **Invalid Type Packets** – Number of VRRP packets received by the virtual router with an invalid value in the "type" field.
- **Error Address List Packets** – Number of packets received for which the address list does not match the locally configured list for the virtual router.
- **Invalid Authentication Type Packets** – Number of packets received with an unknown authentication type.
- **Mismatch Authentication Type Packets** – Number of packets received with "Auth Type" not equal to the locally configured authentication method.
- **Sent Priority 0 Packets** – Number of VRRP packets sent by the virtual router with priority set to 0.

Web – Click IP, VRRP, Group Statistics. Select the VLAN and virtual router group.

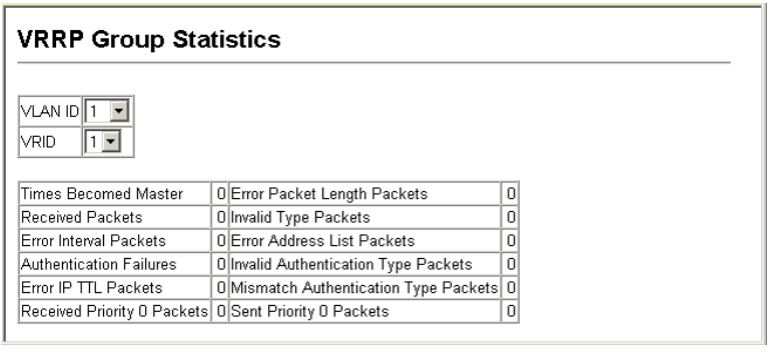

VRRP Group Statistics
VLAN ID 1
VRID 1
Times Becomed Master 0
Received Packets 0
Error Interval Packets 0
Authentication Failures 0
Error IP TTL Packets 0
Received Priority 0 Packets 0
Error Packet Length Packets 0
Invalid Type Packets 0
Error Address List Packets 0
Invalid Authentication Type Packets 0
Mismatch Authentication Type Packets 0
Sent Priority 0 Packets 0

Figure 3-115 VRRP Group Statistics

CLI – This example displays VRRP protocol statistics for group 1, VLAN 1.

```
Console#show vrrp 1 interface vlan 1 counters                    4-391
 Total Number of Times Transitioned to MASTER                        : 6
 Total Number of Received Advertisements Packets                     : 0
 Total Number of Received Error Advertisement Interval Packets       : 0
 Total Number of Received Authentication Failures Packets            : 0
 Total Number of Received Error IP TTL VRRP Packets                  : 0
 Total Number of Received Priority 0 VRRP Packets                    : 0
 Total Number of Sent Priority 0 VRRP Packets                        : 5
 Total Number of Received Invalid Type VRRP Packets                  : 0
 Total Number of Received Error Address List VRRP Packets            : 0
 Total Number of Received Invalid Authentication Type VRRP Packets   : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets  : 0
 Total Number of Received Error Packet Length VRRP Packets           : 0
Console#
```

IP Routing

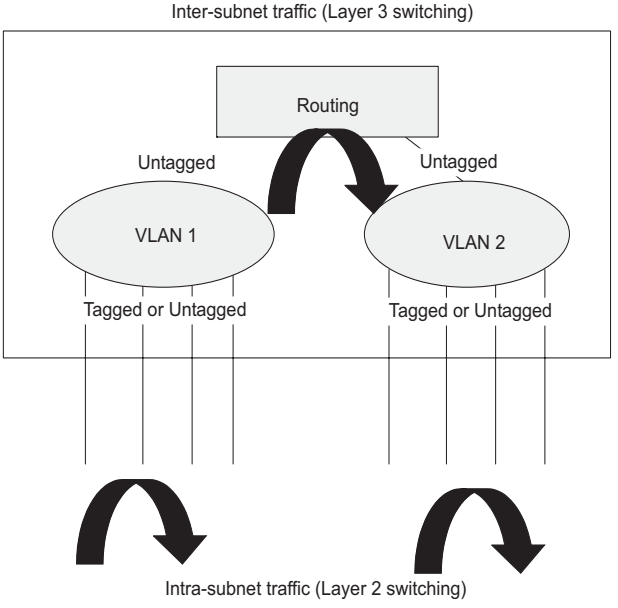
Overview

This switch supports IP routing and routing path management via static routing definitions (page 3-289) and dynamic routing such as RIP (page 3-292) or OSPF (page 3-303). When IP routing is enabled (page 3-293), this switch acts as a wire-speed router, passing traffic between VLANs using different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, no default routing is defined. As with all traditional routers, the routing functions must first be configured to work.

Initial Configuration

In the default configuration, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. Therefore, you should first create VLANs for each unique user group or application traffic (page 3-188), assign all ports that belong to the same group to these VLANs (page 3-190), and then assign an IP interface to each VLAN (page 3-271). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (only as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.



IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
  - Based on the Layer 3 destination address
  - Replacing destination/source MAC addresses for each hop
  - Incrementing the hop count
  - Decrementing the time-to-live
  - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to a router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node via the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

Note: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

Routing Protocols

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

The switch supports RIP, RIP-2 and OSPFv2 dynamic routing protocols.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a

rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

OSPFv2 Dynamic Routing Protocol

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

Non-IP Protocol Routing

The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

Basic IP Interface Configuration

To allow routing between different IP subnets, you must enable IP Routing as described in this section. You also need to you define a VLAN for each IP subnet that will be connected directly to this switch. Note that you must first create a VLAN as described under "Creating VLANs" on page 3-188 before configuring the corresponding subnet. Remember that if you need to manage the switch in-band then you must define the IP subnet address for at least one VLAN.

Command Attributes

- **IP Routing Status** – Configures the switch to operate as a Layer 2 switch or as a multilayer routing switch. (Options: Disable this field to restrict operation to Layer 2 switching; enable it to allow multilayer operation at either Layer 2 or 3 as required.)
  - This command affects both static and dynamic unicast routing.
  - If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.
- **Default Gateway** – The routing device to which the switch will pass packets for all unknown subnets; i.e., packets that do not match any routing table entry. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

Web - Click IP, General, Global Settings. Set IP Routing Status to Disabled to restrict operation to Layer 2, or Enabled to allow multilayer switching, specify the default gateway which will be forwarded packets for all unknown subnets, and click Apply.

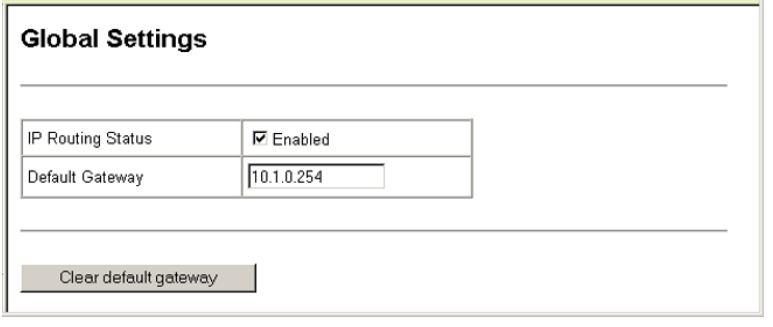


Figure 3-116 IP Global Settings

CLI - This example enables IP routing, and sets the default gateway.

```
Console(config)#ip routing                                    4-318
Console(config)#ip route default 10.1.0.254                   4-319
```

Configuring IP Routing Interfaces

You can specify the IP subnets connected to this router by manually assigning an IP address to each VLAN, or by using the RIP or OSPF dynamic routing protocol to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.
- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4093).
- **IP Address Mode** – Specifies whether the IP address for this interface is statically assigned, or obtained from a network address server. (Options: Static, DHCP - Dynamic Host Configuration Protocol, BOOTP - Boot Protocol; Default: Static)
  - If Static address type is selected, then you must also specify whether the IP address is the primary IP address on the VLAN or a secondary

IP address. An interface can have only one primary IP address, but can have multiple secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can accessed via this interface.

- If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the address server. Requests will be broadcast periodically by the router for an IP address. (DHCP/BOOTP values include the IP address and subnet mask.)

- **IP Address** – Address of the VLAN interface. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

Web - Click IP, General, Routing Interface. Specify an IP interface for each VLAN that will support routing to other subnets. First specify a primary address, and click Set IP Configuration. If you need to assign secondary addresses, enter these addresses one at a time, and click Set IP Configuration after entering each address.

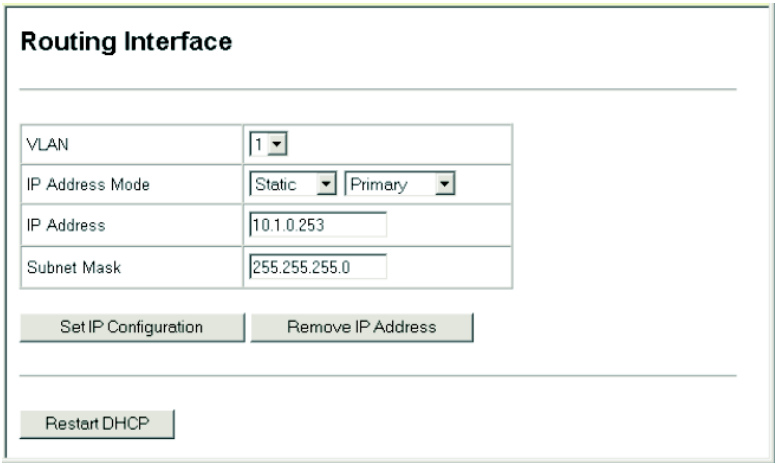


Figure 3-117 IP Routing Interface

CLI - This example sets a primary IP address for VLAN 1, and then adds a secondary IP address for a different subnet also attached to this router interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.253 255.255.255.0        4-308
Console(config-if)#ip address 10.1.9.253 255.255.255.0 secondary
Console(config-if)#
```

Address Resolution Protocol

If IP routing is enabled (page 3-269), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards- based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

Table 3-16 Address Resolution Protocol

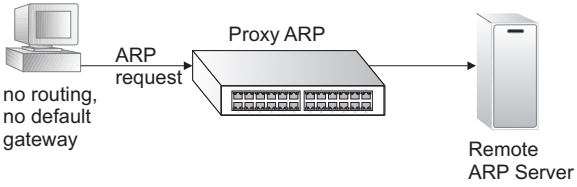
destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC

address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.



Basic ARP Configuration

You can use the ARP General configuration menu to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

Command Usage

- The aging time determines how long dynamic entries remain the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Command Attributes

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)
- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces.

Web - Click IP, ARP, General. Set the timeout to a suitable value for the ARP cache, enable Proxy ARP for subnetworks that do not have routing or a default gateway, and click Apply.

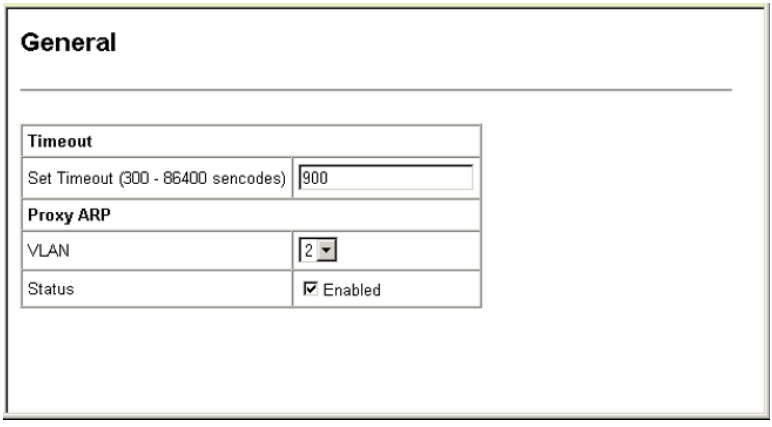


Figure 3-118 ARP General

CLI - This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds), and enables Proxy ARP for VLAN 3.

```
Console(config)#arp-timeout 900                                    4-315
Console(config)#interface vlan 3                                   4-187
Console(config-if)#ip proxy-arp                                    4-316
Console(config-if)#
```

Configuring Static ARP Addresses

For devices that do not respond to ARP requests, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, you can manually map an IP address to the corresponding physical address in the ARP.

Command Usage

- You can define up to 128 static entries in the ARP cache.
- Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.

Command Attributes

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx.)
- **Entry Count** – The number of static entries in the ARP cache.

Web - Click IP, ARP, Static Addresses. Enter the IP address, the corresponding MAC address, and click Apply.

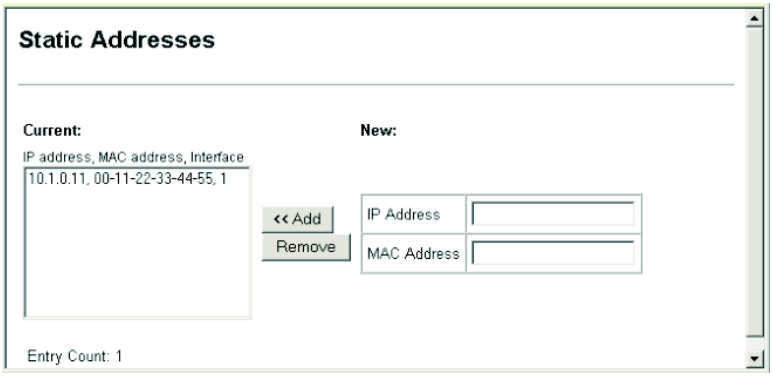


Figure 3-119 ARP Static Addresses

CLI - This example sets a static entry for the ARP cache.

```
Console(config)#arp 10.1.0.11 00-11-22-33-44-55                    4-314
Console(config)#
```

Displaying Dynamically Learned ARP Entries

The ARP cache contains entries that map IP addresses to the corresponding physical address. Most of these entries will be dynamically learned through replies to broadcast messages. You can display all of the dynamic entries in the ARP cache, change specific dynamic entries into static entries, or clear all dynamic entries from the cache.

Command Attributes

- **IP Address** – IP address of a dynamic entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Dynamic to Static**[22] – Changes a selected dynamic entry to a static entry.

22. These buttons take effect immediately. You are not prompted to confirm the action.

- **Clear All** – Deletes all dynamic entries from the ARP cache.
- **Entry Count** – The number of dynamic entries in the ARP cache.

Web - Click IP, ARP, Dynamic Addresses. You can use the buttons provided to change a dynamic entry to a static entry, or to clear all dynamic entries in the cache.



Figure 3-120 ARP Dynamic Addresses

CLI - This example shows all entries in the ARP cache.

```
Console#show arp                                                    4-316
Arp cache timeout: 1200 (seconds)

    IP Address       MAC Address      Type    Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other           1
      10.1.0.11 00-11-22-33-44-55    static           1
      10.1.0.12 01-02-03-04-05-06    static           1
      10.1.0.19 00-10-b5-62-03-74   dynamic           1
     10.1.0.253 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1

Total entry : 6
Console#clear arp-cache                                             4-315
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

Displaying Local ARP Entries

The ARP cache also contains entries for local interfaces, including subnet, host, and broadcast addresses.

Command Attributes

- **IP Address** – IP address of a local entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Entry Count** – The number of local entries in the ARP cache.

Web - Click IP, ARP, Other Addresses.

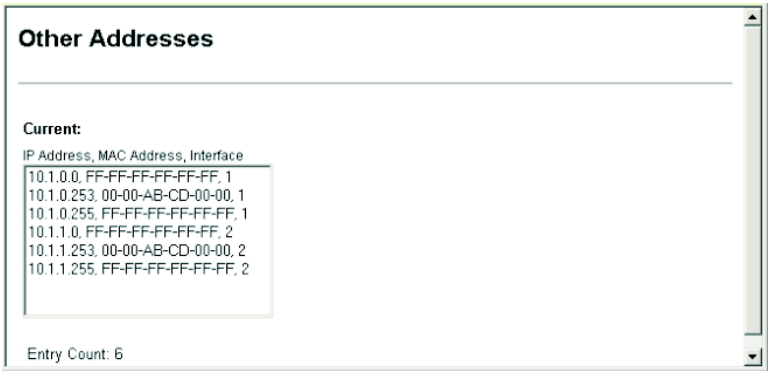


Figure 3-121 ARP Other Addresses

CLI - This router uses the Type specification "other" to indicate local cache entries in the ARP cache.

```
Console#show arp                                                    4-316
Arp cache timeout: 1200 (seconds)

    IP Address        MAC Address       Type    Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other           1
      10.1.0.11 00-11-22-33-44-55    static           1
      10.1.0.12 01-02-03-04-05-06    static           1
      10.1.0.19 00-10-b5-62-03-74   dynamic           1
     10.1.0.253 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1

Total entry : 6
Console#
```

Displaying ARP Statistics

You can display statistics for ARP messages crossing all interfaces on this router.

Table 3-17 ARP Statistics

Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

Web - Click IP, ARP, Statistics.



Figure 3-122 ARP Statistics

CLI - This example provides detailed statistics on common IP-related protocols.

```
Console#show ip traffic                                          4-323
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#
```

Displaying Statistics for IP Protocols

IP Statistics

The Internet Protocol (IP) provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (i.e., hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.

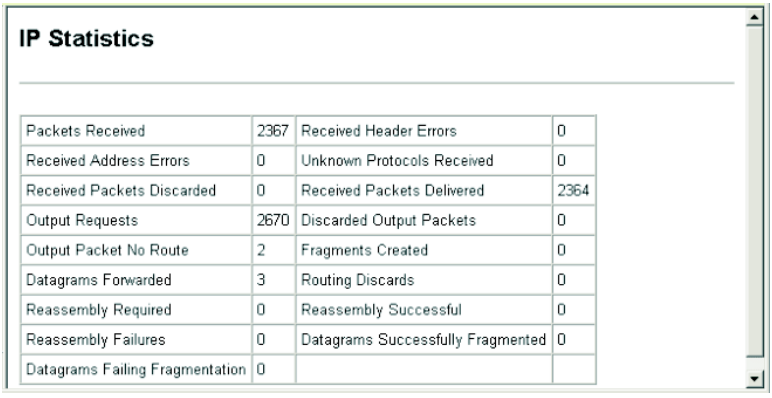
Table 3-18 IP Statistics

Parameter	Description
Packets Received	The total number of input datagrams received from interfaces, including those received in error.
Received Address Errors	The number of input datagrams discarded because the IP address in the header's destination field was not a valid address for this entity.
Received Packets Discarded	The number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).
Output Requests	The total number of datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
Output Packet No Route	The number of datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
Datagrams Forwarded	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
Reassembly Required	The number of IP fragments received which needed to be reassembled at this entity.

Table 3-18 IP Statistics (Continued)

Parameter	Description
Reassembly Failures	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.).
Datagrams Failing Fragmentation	The number of datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their "Don't Fragment" flag was set.
Received Header Errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Unknown Protocols Received	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Received Packets Delivered	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Discarded Output Packets	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).
Fragments Created	The number of datagram fragments that have been generated as a result of fragmentation at this entity.
Routing Discards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
Reassembly Successful	The number of datagrams successfully re-assembled.
Datagrams Successfully Fragmented	The number of IP datagrams that have been successfully fragmented at this entity.

Web - Click IP, Statistics, IP.



IP Statistics

Packets Received	2367	Received Header Errors	0
Received Address Errors	0	Unknown Protocols Received	0
Received Packets Discarded	0	Received Packets Delivered	2364
Output Requests	2670	Discarded Output Packets	0
Output Packet No Route	2	Fragments Created	0
Datagrams Forwarded	3	Routing Discards	0
Reassembly Required	0	Reassembly Successful	0
Reassembly Failures	0	Datagrams Successfully Fragmented	0
Datagrams Failing Fragmentation	0		

Figure 3-123 IP Statistics

CLI - See the example on page 3-280.

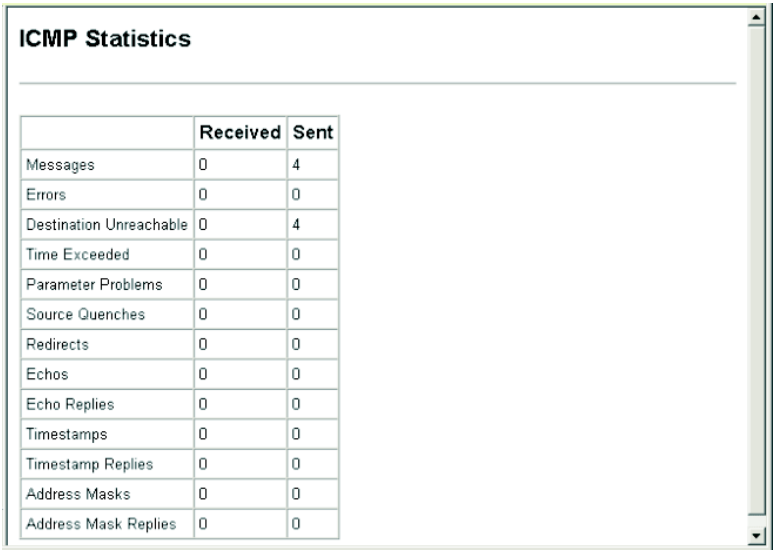
ICMP Statistics

Internet Control Message Protocol (ICMP) is a network layer protocol that transmits message packets to report errors in processing IP packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (i.e., the next hop router) to use for a specific destination.

Table 3-19 ICMP Statistics

Parameter	Description
Messages	The total number of ICMP messages which the entity received/sent.
Errors	The number of ICMP messages which the entity received/sent but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
Destination Unreachable	The number of ICMP Destination Unreachable messages received/sent.
Time Exceeded	The number of ICMP Time Exceeded messages received/sent.
Parameter Problems	The number of ICMP Parameter Problem messages received/sent.
Source Quenches	The number of ICMP Source Quench messages received/sent.
Redirects	The number of ICMP Redirect messages received/sent.
Echos	The number of ICMP Echo (request) messages received/sent.
Echo Replies	The number of ICMP Echo Reply messages received/sent.
Timestamps	The number of ICMP Timestamp (request) messages received/sent.
Timestamp Replies	The number of ICMP Timestamp Reply messages received/sent.
Address Masks	The number of ICMP Address Mask Request messages received/sent.
Address Mask Replies	The number of ICMP Address Mask Reply messages received/sent.

Web - Click IP, Statistics, ICMP.



ICMP Statistics

	Received	Sent
Messages	0	4
Errors	0	0
Destination Unreachable	0	4
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echos	0	0
Echo Replies	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

Figure 3-124 ICMP Statistics

CLI - See the example on page 3-280.

UDP Statistics

User Datagram Protocol (UDP) provides a datagram mode of packet-switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Table 3-20 USP Statistics

Parameter	Description
Datagrams Received	The total number of UDP datagrams delivered to UDP users.
Datagrams Sent	The total number of UDP datagrams sent from this entity.
Receive Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Web - Click IP, Statistics, UDP.

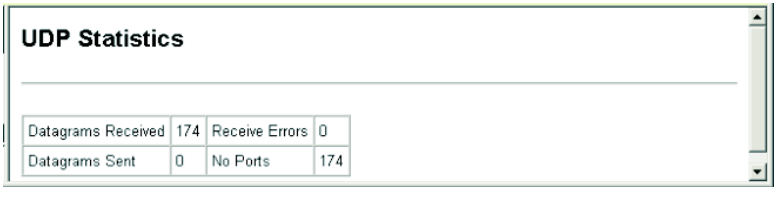


Figure 3-125 UDP Statistics

CLI - See the example on page 3-280.

TCP Statistics

The Transmission Control Protocol (TCP) provides highly reliable host-to-host connections in packet-switched networks, and is used in conjunction with IP to support a wide variety of Internet protocols.

Table 3-21 TCP Statistics

Parameter	Description
Segments Received	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Segments Sent	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Failed Connection Attempts	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Current Connections	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Receive Errors	The total number of segments received in error (e.g., bad TCP checksums).
Segments Retransmitted	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Reset Connections	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Web - Click IP, Statistics, TCP.

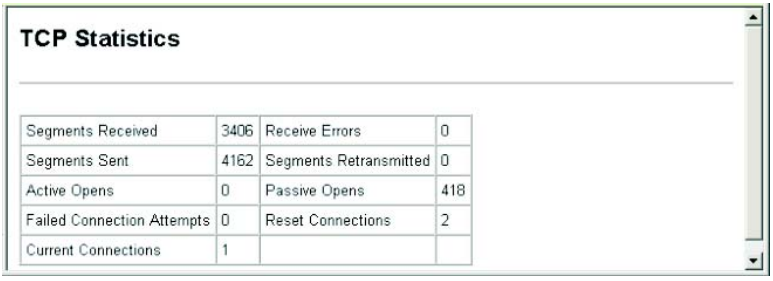

TCP Statistics
Segments Received 3406 Receive Errors 0
Segments Sent 4162 Segments Retransmitted 0
Active Opens 0 Passive Opens 418
Failed Connection Attempts 0 Reset Connections 2
Current Connections 1

Figure 3-126 TCP Statistics

CLI - See the example on page 3-280.

Configuring Static Routes

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP or OSPF). However, you can also manually enter static routes in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Gateway** – IP address of the gateway used for this route.
- **Metric** – Cost for this interface. This cost is only used if a route is imported by a dynamic routing protocol such as OSPF. (Range: 1-5, default: 1)
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Static Routes.

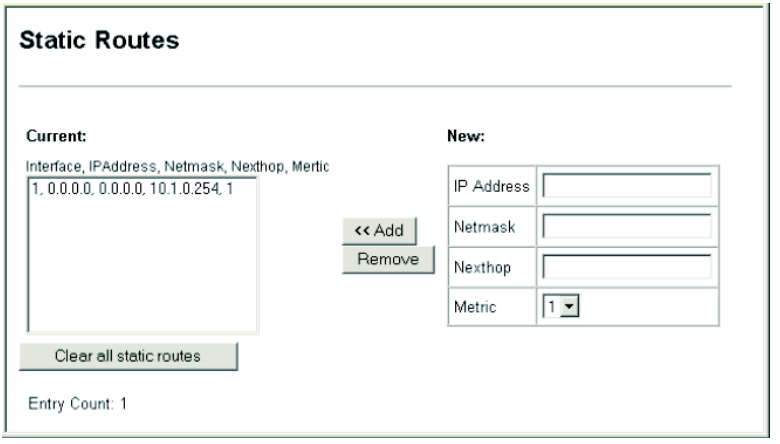


Figure 3-127 IP Static Routes

CLI - This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0
  192.168.5.254                                          4-319
Console(config)#
```

Displaying the Routing Table

You can display all the routes that can be accessed via the local network interfaces, via static routes, or via a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic. Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

Command Attributes

- **Interface** – Index number of the IP interface.

- **IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – The IP address of the next hop (or gateway) in this route.
- **Protocol** – The protocol which generated this route information. (Options: local, static, RIP, OSPF)
- **Metric** – Cost for this interface.
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Routing Table.

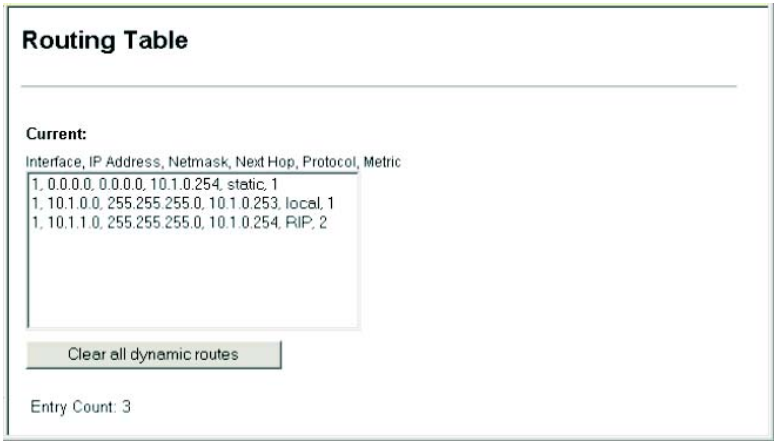

Routing Table
Current:
Interface, IP Address, Netmask, Next Hop, Protocol, Metric
1, 0.0.0.0, 0.0.0.0, 10.1.0.254, static, 1
1, 10.1.0.0, 255.255.255.0, 10.1.0.253, local, 1
1, 10.1.1.0, 255.255.255.0, 10.1.0.254, RIP, 2
Clear all dynamic routes
Entry Count: 3

Figure 3-128 IP Routing Table

CLI - This example shows routes obtained from various methods.

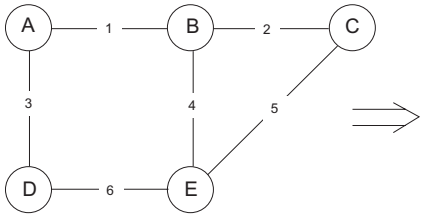
```
Console#show ip route                                          4-320

  Ip Address        Netmask         Next Hop     Protocol Metric Interface
--------------- --------------- --------------- -------- ------ ---------
        0.0.0.0         0.0.0.0      10.1.0.254   static      1         1
       10.1.0.0   255.255.255.0      10.1.0.253    local      1         1
       10.1.1.0   255.255.255.0      10.1.0.254      RIP      2         1

Total entries: 3
Console#
```

Configuring the Routing Information Protocol

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.



Cost = 1 for all links

A	Link	Cost
A	0	0
B	1	1
C	1	2
D	3	1
E	1	2

Routing table for node A

Command Usage

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:
  - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
  - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
  - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.
- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

- There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

Configuring General Protocol Settings

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (page 3-296).

Command Usage

- When you specify a Global RIP Version, any VLAN interface not previously set to a specific Receive or Send Version (page 3-296) is set to the following values:
  - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- The *update* timer is the fundamental timer used to control all basic RIP processes.
  - Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.
  - The timers must be set to the same values for all routers in the network.

Command Attributes

Global Settings

- **RIP Routing Process** – Enables RIP routing for all IP interfaces on the router. (Default: Disabled)
- **Global RIP Version** – Specifies a RIP version used globally by the router. (Default: RIP Version 1)

Timer Settings

- **Update** – Sets the rate at which updates are sent. This value will also set the timeout timer to 6 times the update time, and the garbage-collection timer to 4 times the update time. (Range: 15-60 seconds; Default: 30 seconds)
- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. (Default: 180 seconds)
- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. (Default: 120 seconds)

Web - Click Routing Protocol, RIP, General Settings. Enable or disable RIP, set the RIP version used on previously unset interfaces to RIPv1 or RIPv2, set the basic update timer, and then click Apply.

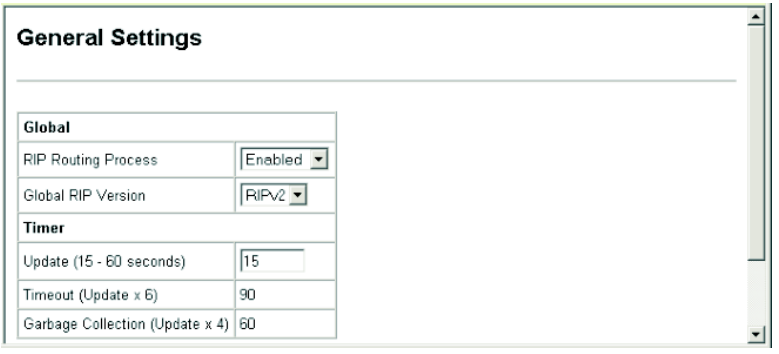


Figure 3-129 RIP General Settings

CLI - This example sets the router to use RIP Version 2, and sets the basic timer to 15 seconds.

```
Console(config)#router rip                                    4-325
Console(config-router)#version 2                              4-328
Console(config-router)#timers basic 15                        4-325
Console(config-router)#end
Console#show rip globals                                      4-335

RIP Process: Enabled
Update Time in Seconds: 15
Number of Route Change: 0
Number of Queries: 1
Console#
```

Specifying Network Interfaces for RIP

You must specify network interfaces that will be included in the RIP routing process.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:
  - 0 - 127 is class A, and only the first field in the network address is used.
  - 128 - 191 is class B, and the first two fields in the network address are used.
  - 192 - 223 is class C, and the first three fields in the network address are used.

Command Attributes

Subnet Address – IP address of a network directly connected to this router.

Web - Click Routing Protocol, RIP, Network Addresses. Add all interfaces that will participate in RIP, and click Apply.

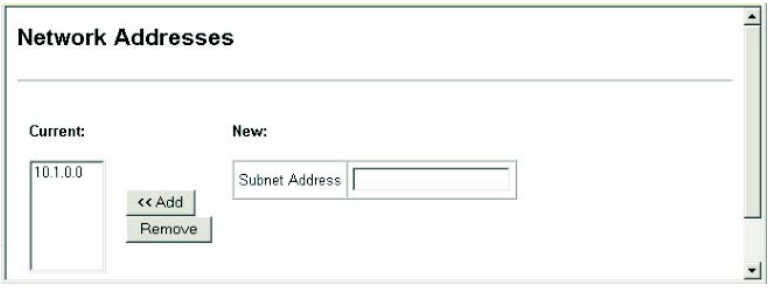


Figure 3-130 RIP Network Addresses

CLI - This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config)#router-rip                                          4-325
Console(config-router)#network 10.1.0.0                             4-327
Console(config-router)#end
Console#show ip rip status                                          4-336

          Peer   UpdateTime   Version   RcvBadPackets   RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.253              0               0               73
     10.1.1.253              0               0               66

Console#
```

Configuring Network Interfaces for RIP

For each interface that participates in the RIP routing process, you must specify the protocol message type accepted (i.e., RIP version) and the message type sent (i.e., RIP version or compatibility mode), the method for preventing loopback of protocol messages, and whether or not authentication is used (i.e., authentication only applies if RIPv2 messages are being sent or received).

Command Usage

Specifying Receive and Send Protocol Types

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified by the RIP / General Settings, Global RIP Version field.
- You can specify the Receive Version based on these options:
  - Use "RIPv1" or "RIPv2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "RIPv1 or RIPv2" if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.
  - Use "Do Not Receive" if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
- You can specify the Send Version based on these options:
  - Use "RIPv1" or "RIPv2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "RIPv1 Compatible" to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)
  - Use "Do Not Send" to passively monitor route information advertised by other routers attached to the network.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP utilizes the following

three methods that can provide faster convergence when the network topology changes and prevent most loops from occurring:

- Split Horizon – Never propagate routes back to an interface port from which they have been acquired.
- Poison Reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- Triggered Updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required. RIPv2 supports authentication via a simple password. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4093).
- **Receive Version** – The RIP version to receive on an interface.
  - **RIPv1**: Accepts only RIPv1 packets.
  - **RIPv2**: Accepts only RIPv2 packets.
  - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets. (Default)
  - **Do Not Receive**: Does not accept incoming RIP packets.

  (The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 or RIPv2 packets, RIPv2 - RIPv2 packets)

- **Send Version** – The RIP version to send on an interface.
  - **RIPv1**: Sends only RIPv1 packets.
  - **RIPv2**: Sends only RIPv2 packets.
  - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2. (Default)
  - **Do Not Send**: Does not transmit RIP updates.

  (The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 Compatible, RIPv2 - RIPv2 packets)
- **Instability Preventing** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router. (Default: Split Horizon)
  - **None**: No method is used. If a loop occurs, the hop count for a route may be gradually incremented to infinity (i.e., 16) before the route is deemed unreachable.
  - **Split Horizon**: This method never propagates routes back to an interface from which they have been acquired.
  - **Poision Reverse**: This method propagates routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- **Authentication Type** – Specifies whether or not authentication is required for exchanging protocol messages. (Default: No Authentication)
  - **No Authentication**: No authentication is required.
  - **Simple Password**: Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

Web - Click Routing Protocol, RIP, Interface Settings. Select the RIP protocol message types that will be received and sent, the method used to provide faster convergence and prevent loopback (i.e., prevent instability in the network topology), and the authentication option and corresponding password. Then click Apply.

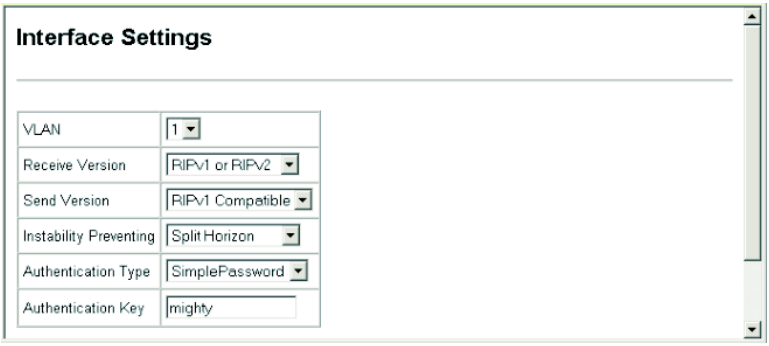


Figure 3-131 RIP Interface Settings

CLI - This example sets the receive version to accept both RIPv1 or RIPv2 messages, the send mode to RIPv1 compatible (i.e., called v2-broadcast in the CLI), sets the method of preventing instability in the network topology to Split Horizon, enables authentication via a simple password (i.e., called text mode in the CLI).

```
Console(config)#interface vlan 1                                    4-187
Console(config-if)#ip rip receive version 1 2                       4-330
Console(config-if)#ip rip send version v2-broadcast                 4-331
Console(config-if)#ip split-horizon                                 4-332
Console(config-if)#ip rip authentication mode text                  4-334
Console(config-if)#ip rip authentication key mighty                 4-333
Console#
```

Displaying RIP Information and Statistics

You can display basic information about the current global configuration settings for RIP, statistics about route changes and queries, information about the interfaces on this router that are using RIP, and information about known RIP peer devices.

Table 3-22 RIP Information and Statistics

Parameter	Description
Globals	
RIP Routing Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.
Interface Information	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, rip1Compatible).
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1Orv2).
InstabilityPreventing	Shows if split-horizon, poison-reverse, or no instability prevention method is in use.
AuthType	Shows if authentication is set to simple password or none.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
Peer Information	
PeerAddress	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Web - Click Routing Protocol, RIP, Statistics.

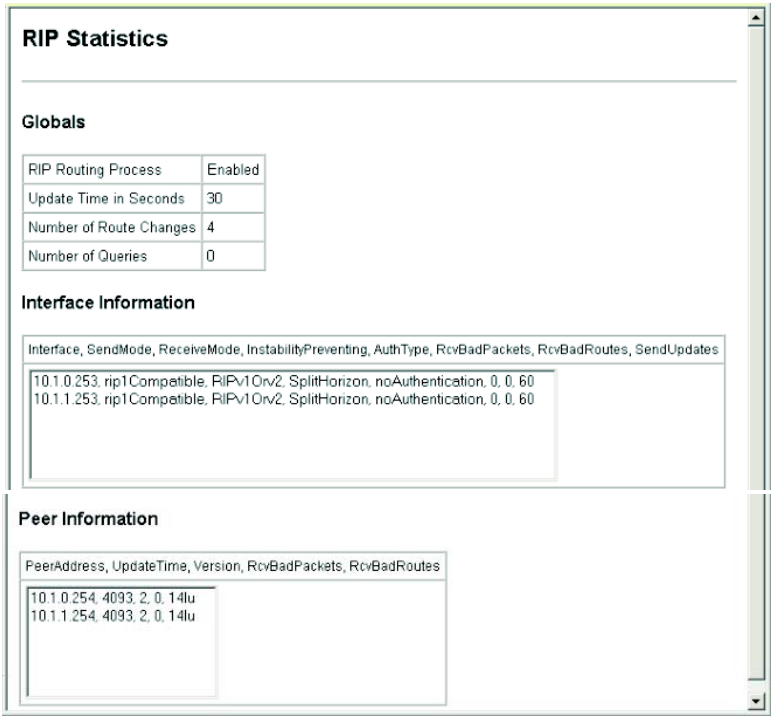


Figure 3-132 RIP Statistics

CLI - The information displayed by the RIP Statistics screen via the web interface can be accessed from the CLI using the following commands.

```
Console#show rip globals                                              4-335

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 4
Number of Queries: 0
Console#show ip rip configuration                                     4-336

     Interface      SendMode      ReceiveMode     Poison       Authentication
-------------- --------------- ------------- -------------- ------------------
     10.1.0.253  rip1Compatible     RIPv1Orv2   SplitHorizon   noAuthentication
     10.1.1.253  rip1Compatible     RIPv1Orv2   SplitHorizon   noAuthentication
Console#show ip rip status                                            4-336

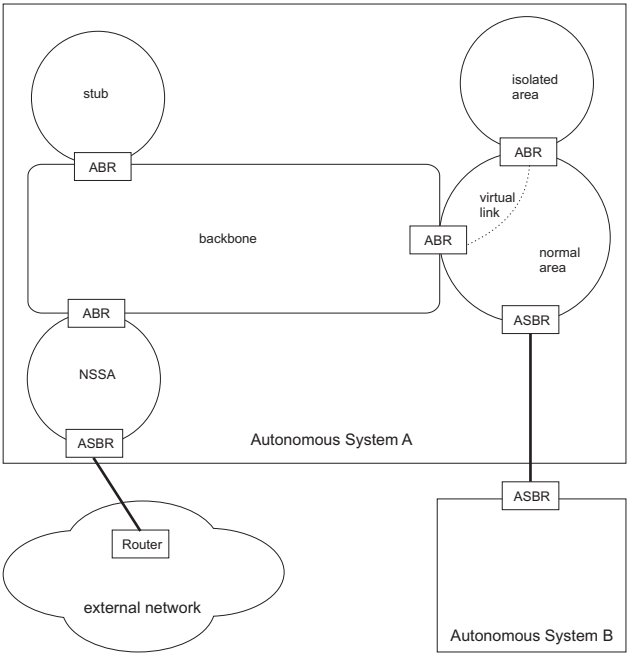
     Interface   RcvBadPackets   RcvBadRoutes     SendUpdates
-------------- --------------- -------------- ---------------
     10.1.0.253               0              0              60
     10.1.1.253               0              0              63
Console#show ip rip peer                                              4-336

          Peer   UpdateTime   Version   RcvBadPackets   RcvBadRoutes
-------------- ------------ --------- --------------- --------------
     10.1.0.254         4610         2               0              0
     10.1.1.254         4610         2               0              0
Console#
```

Configuring the Open Shortest Path First Protocol

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

Note: The OSPF protocol implemented in this device is based on Version 2 (RFC 2328). It also supports Version 1 (RFC 1583) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older OSPF routers exist; as well as the not-so-stubby area option (RFC 1587).



Command Usage

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.
- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.

- When using OSPF, you must organize your network (i.e., autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSFP backbone.
  - To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.
  - You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).
  - And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

Configuring General Protocol Settings

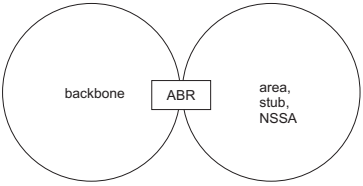
To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached, then use the OSPF / General Configuration menu to enable OSPF, assign an Router ID to this device, and set the other basic protocol parameters.

Command Attributes

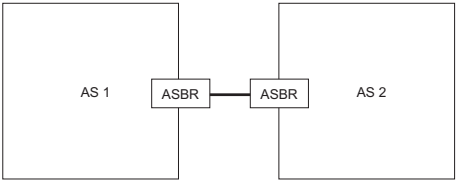
General Information –

- **OSPF Routing Process** – Enables or disables OSPF routing for all IP interfaces on the router. (Default: Disabled)
- **OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system. (Default: The lowest interface address)

- **Version Number** [23] – This router only supports OSPF Version 2.
- **Area Border Router** – Indicates if this router connect directly to networks in two or more areas. An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area.



- **AS Boundary Router** [24] Allows this router to exchange routing information with boundary routers in other autonomous systems to which it may be attached. If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device. (Default: Disabled)



- **Rfc1583 Compatible** – If one or more routers in a routing domain are using OSPF Version 1, this router should use RFC 1583 (OSPFv1) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)
- **SPF Hold Time (seconds)** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535; Default: 10)
- **Area Numbers** – The number of OSPF areas configured on this router.

23. These items are read only.
24. CLI - These are configured with the **default-information originate** command (page 4-342).

Default Route Information –

- **Originate Default Route** – Generates a default external route into an autonomous system. Note that the **AS Boundary Router** field must be enabled, and the **Advertise Default Route** field properly configured. (Default: Disabled)
- **Advertise Default Route** – The router can advertise a default external route into the autonomous system (AS). (Options: NotAlways, Always; Default: NotAlways)
  - **Always** – The router will advertise itself as a default external route for the AS, even if a default external route does not actually exist.
  - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes via RIP or static configuration, and such a route is known. (See "Redistributing External Routes" on page 3-327.)
- **External Metric Type** – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)
- **Default External Metric** – The Metric assigned to the default route. (Range: 1-65535; Default: 10)

Web - Click Routing Protocol, OSPF, General Configuration. Enable OSPF, specify the Router ID, configure the other global parameters as required, and click Apply.

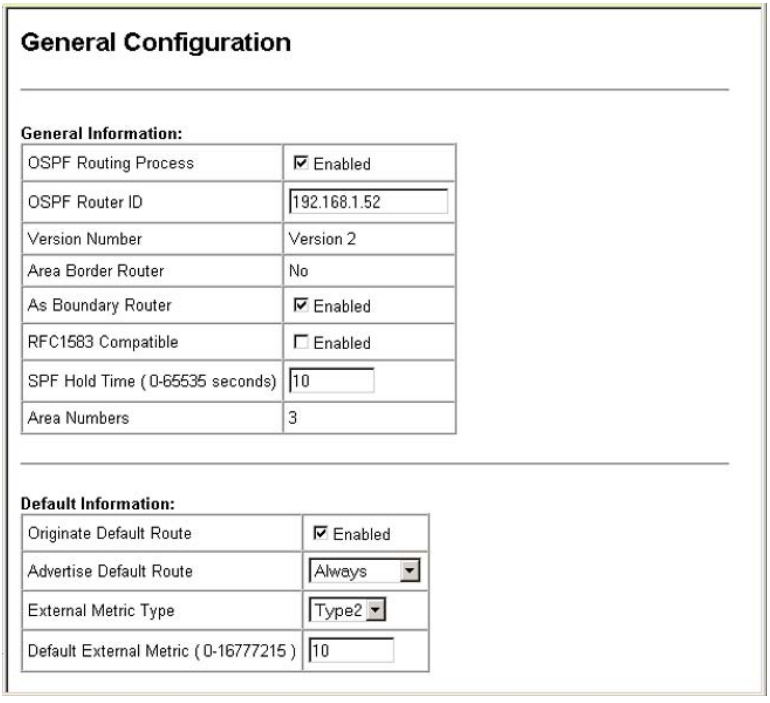


Figure 3-133 OSPF General Configuration

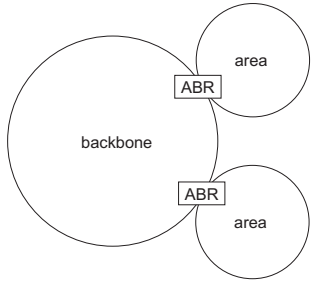
CLI - This example configures the router with the same settings as shown in the screen capture for the web interface.

```
Console(config)#router ospf                                    4-340
Console(config-router)#router-id 10.1.1.253                    4-340
Console(config-router)#no compatible rfc1583                   4-341
Console(config-router)#default-information originate always
  metric 10 metric-type 2                                      4-342
Console(config-router)#timers spf 10                           4-343
Console(config-router)#
```

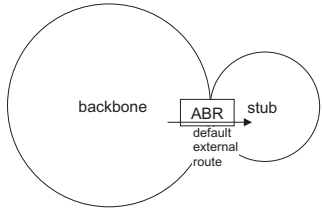
Configuring OSPF Areas

An autonomous system must be configured with a backbone area, designated by area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, you can configure an area to export a single summarized route that covers a broad range of network addresses within the area (page 3-313). To further reduce the amount of routes passed between areas, you can configure an area as a stub or a not-so-stubby area (NSSA).



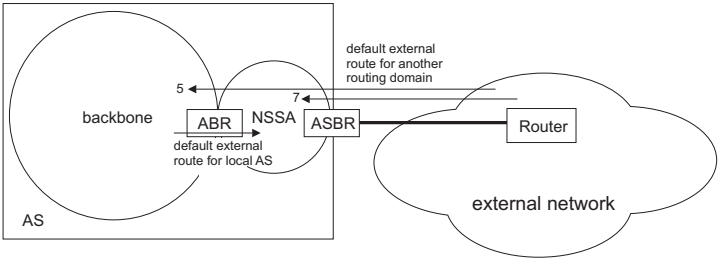
Normal Area – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.



Stub – A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.

- By default, a stub can only pass traffic to other areas in the autonomous system via the default external route. However, you also can configure an area border router to send Type 3 summary link advertisements into the stub.

NSSA – A not-so-stubby area (NSSA) is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS). However, an NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by area border routers. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.



- Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned via OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.

Default Cost – This specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR).

Command Usage

- Before you create a stub or NSSA, first specify the address range for an area using the Network Area Address Configuration screen (page 3-323).
- Stubs and NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- A stub or NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

Command Attributes

- **Area ID** – Identifier for an area, stub or NSSA.
- **Area Type** – Specifies a normal area, stub area, or not-so-stubby area (NSSA). Area ID 0.0.0.0 is set to the backbone by default. (Default: Normal area)
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 1)
  - Note that if you set the default cost to "0," the router will not advertise a default route into the attached stub.
- **Summary** – Makes an ABR send a Type-3 summary link advertisement into a stub. (Default: Summary)
  - A stub is designed to save routing table space by blocking Type-4 AS summary LSAs and Type 5 external LSAs. If you use the "NoSummary" option to also block Type-3 summary LSAs that advertise the default route for destinations external to the local area or the AS, the stub will become completely isolated.

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Area Configuration. Set any area to a stub or NSSA as required, specify the cost for the default summary route sent into a stub, and click Apply.

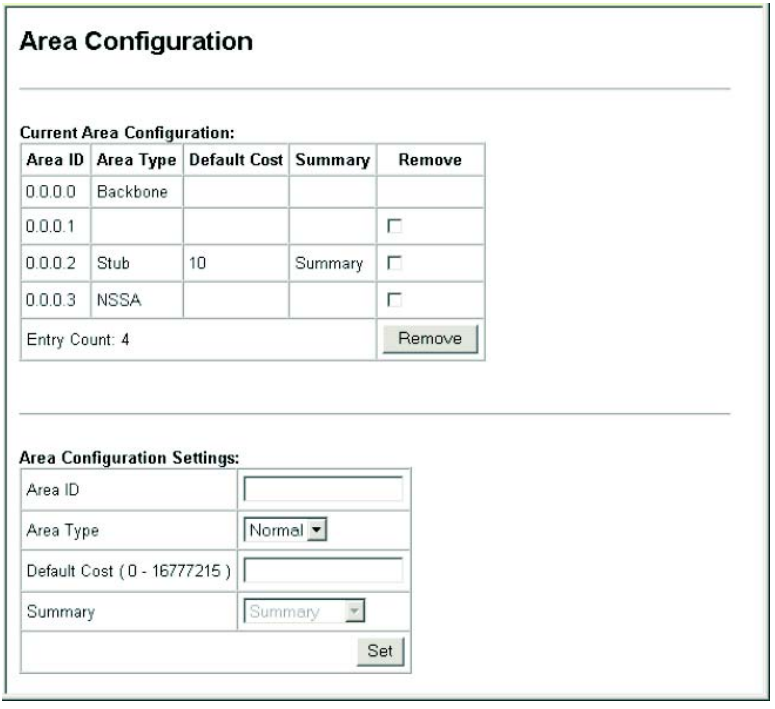


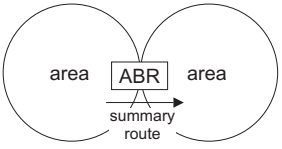
Figure 3-134 OSPF Area Configuration

CLI - This example configures area 0.0.0.1 as a normal area, area 0.0.0.2 as a stub, and area 0.0.0.3 as an NSSA. It also configures the router to propagate a default summary route into the stub and sets the cost for this default route to 10.

```
Console(config-router)#network 10.1.1.0 255.255.255.0
  area 0.0.0.1                                              4-348
Console(config-router)#area 0.0.0.2 stub summary            4-350
Console(config-router)#area 0.0.0.2 default-cost 10         4-345
Console(config-router)#area 0.0.0.3 nssa                    4-351
Console(config-router)#end
```

```
Console#show ip ospf                                          4-364
Routing Process with ID 192.168.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 3
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 40 times
Area 0.0.0.2 (STUB)
     Number of interfaces in this area is 1
     SPF algorithm executed 8 times
Area 0.0.0.3 (NSSA)
     Number of interfaces in this area is 1
     SPF algorithm executed 40 times
Console#
```

Configuring Area Ranges (Route Summarization for ABRs)



An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

Command Usage

- Use the Area Range Configuration page to summarize the routes for an area. The summary route for an area is defined by an IP address and network mask. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. This router also supports Variable Length Subnet Masks (VLSMs), so you can summarize an address range on any bit boundary in a network address.
- To summarize the external LSAs imported into your autonomous system (i.e., local routing domain), use the Summary Address Configuration screen (page 3-325).

Command Attributes

- **Area ID** – Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route. If the summary is not sent, the routes remain hidden from the rest of the network. (Default: Advertise)

Note: This router supports up 64 summary routes for area ranges.

Web - Click Routing Protocol, OSPF, Area Range Configuration. Specify the area identifier, the base address and network mask, select whether or not to advertise the summary route to other areas, and then click Apply.

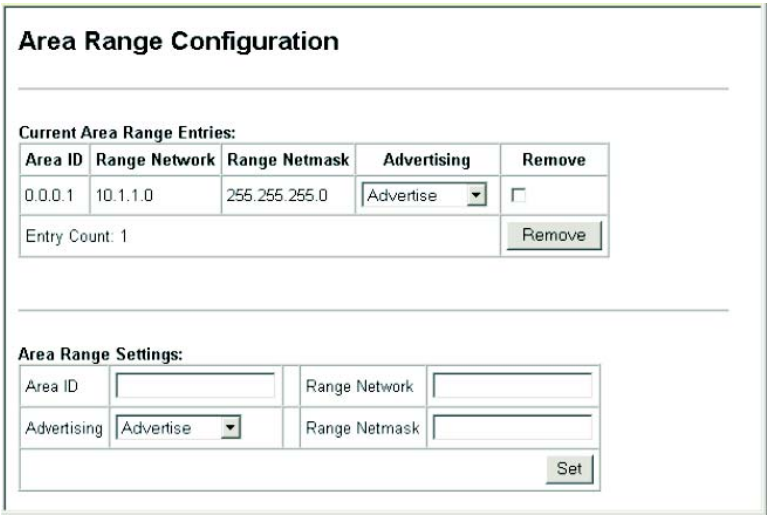


Figure 3-135 OSPF Range Configuration

CLI - This example summarizes all the routes for area 1. Note that the default for the **area range** command is to advertise the route summary. The configured summary route is shown in the list of information displayed for area 1.

```
Console(config-router)#area 0.0.0.1 range 10.1.1.0 255.255.255.0
4-348
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 0
     SPF algorithm executed 47 times
Area 0.0.0.1
     Number of interfaces in this area is 3
     SPF algorithm executed 14 times
     Area ranges are
        255.255.255.0/24  Active
Console#
```

Configuring OSPF Interfaces

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (i.e., one primary interface and one or more secondary interfaces), and then use the OSPF / Network Area Address Configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, you need to use the OSPF / Interface Configuration page to configure the interface-specific parameters used by OSPF to select the designated router, control the timing of link state advertisements, set the cost used to select preferred paths, and specify the method used to authenticate routing messages.

Field Attributes

OSPF Interface List

- **VLAN ID** – The VLAN to which an IP interface has been assigned.
- **Interface IP** – The IP interface associated with the selected VLAN.
- **Area ID** – The area to which this interface has been assigned.
- **Designated Router** – Designated router for this area.
- **Backup Designated Router** – Designated backup router for this area.
- **Entry Count** – The number of IP interfaces assigned to this VLAN.

Note: This router supports up 64 OSPF interfaces.

Detail Interface Configuration

- **VLAN ID** – The VLAN corresponding to the selected interface.
- **Rtr Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)
  - A designated router (DR) and backup designated router (BDR) is elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
  - The router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same priority, the router with the higher ID will be elected. You can set the priority to zero to prevent a router from being elected as a DR or BDR.
  - If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1)
  - LSAs have their age incremented by a delay before transmission. You should consider both the transmission and propagation delays for an

interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.
  - The transmit delay must be the same for all routers in an autonomous system.
  - On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.
- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 1)
  - A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
  - Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.
- **Hello Interval** – Sets the interval between sending hello packets on an interface. (Range: 1-65535 seconds; Default: 10)
  - This interval must be set to the same value for all routers on the network.
  - Using a smaller Hello interval allows changes in the network topology to be discovered more quickly, but may result in more routing traffic.
- **Rtr Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)
- **Cost** – Sets the cost of sending a packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)
  - This router uses a default cost of 1 for all ports. Therefore, if you install a Gigabit module, you need to reset the cost for all of the 100 Mbps ports to some value greater than 1.

- Routes are subsequently assigned a metric equal to the sum of all metrics for each interface link in the route.

- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple password, MD5; Default: None)
  - Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key.
  - When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
  - When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the prespecified target message digest.
  - The Authentication Key and Message Digest Key-id must be used consistently throughout the autonomous system. (Note that the Message Digest Key-id field is disabled when this authentication type is selected.)
- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)
  - You can assign a unique password to each network (i.e., autonomous system) to improve the security of the routing database. However, the password must be used consistently on all neighboring routers throughout a network.
- **Message Digest Key-id** – Assigns a key-id used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)
  - Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate

incoming packets. Neighbor routers must use the same key identifier and key value.

- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Web - Click Routing Protocol, OSPF, Interface Configuration. Select the required interface from the scroll-down box, and click Detailed Settings.

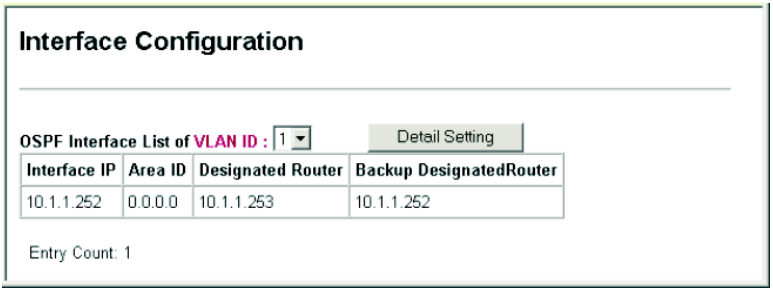


Figure 3-136 OSPF Interface Configuration

Change any of the interface-specific protocol parameters, and then click Apply.

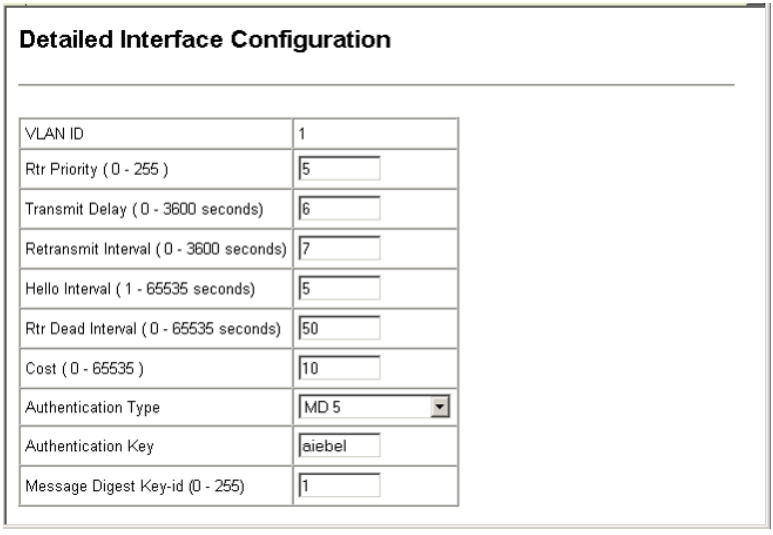
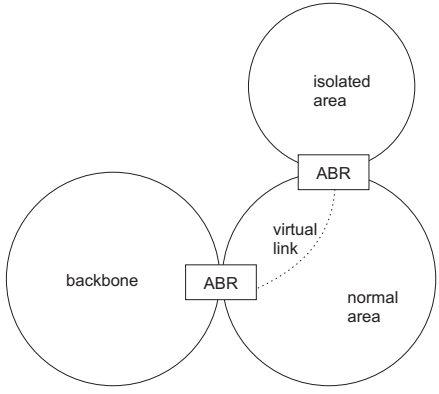


Figure 3-137 OSPF Interface Configuration - Detailed

CLI - This example configures the interface parameters for VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5                          4-361
Console(config-if)#ip ospf transmit-delay 6                    4-363
Console(config-if)#ip ospf retransmit-interval 7               4-362
Console(config-if)#ip ospf hello-interval 5                    4-361
Console(config-if)#ip ospf dead-interval 50                    4-360
Console(config-if)#ip ospf cost 10                             4-359
Console(config-if)#ip ospf authentication message-digest       4-356
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel     4-358
Console#
```

Configuring Virtual Links



All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e., transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR as the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub or NSSA area.)

Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Command Attributes

- **Area ID** – Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- **Neighbor Router ID** – Neighbor router at other end of the virtual link. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area for the virtual link.
- **Events** – The number of state changes or error events on this virtual link.

The other items are described under "Configuring OSPF Interfaces," page 3-315.

Note: This router supports up 64 virtual links.

Web - Click Routing Protocol, OSPF, Virtual Link Configuration. To create a new virtual link, specify the Area ID and Neighbor Router ID, configure the link attributes, and click Add. To modify the settings for an existing link, click the Detail button for the required entry, modify the link settings, and click Set.

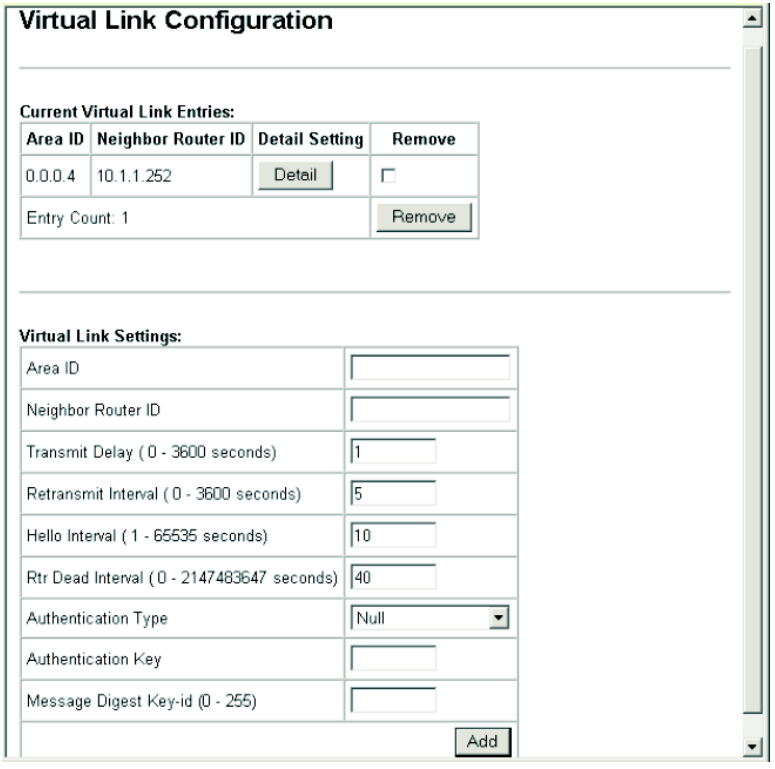


Figure 3-138 OSPF Virtual Link Configuration

CLI - This example configures a virtual link from the ABR adjacent to area 0.0.0.4, through a transit area to the neighbor router 10.1.1.252 at the other end of the link which is adjacent to the backbone.

```
Console(config-router)#area 0.0.0.0 virtual-link 10.1.1.252   4-353
Console(config-router)#
```

Configuring Network Area Addresses

OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Command Usage

- Use the Network Area Address Configuration page to specify an Area ID and the corresponding network address range. Each area identifies a logical group of OSPF routers that actively exchange LSAs to ensure that they share an identical view of the network topology.
- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. The default value 0.0.0.0 is used as the Area ID for the backbone. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.
- An area initially configured via the Network Area Address Configuration page is set as a normal area (or transit area) by default. A normal area can send and receive external Link State Advertisements (LSAs). If necessary, you can use the Area Configuration page to configure an area as a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area (page 3-309).
- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network (page 3-313).

Command Attributes

- **IP Address** – Address of the interfaces to add to the area.
- **Netmask** – Network mask of the address range to add to the area.
- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Network Area Address Configuration. Configure a backbone area that is contiguous with all the other areas in your network, configure an area for all of the other OSPF interfaces, then click Apply.

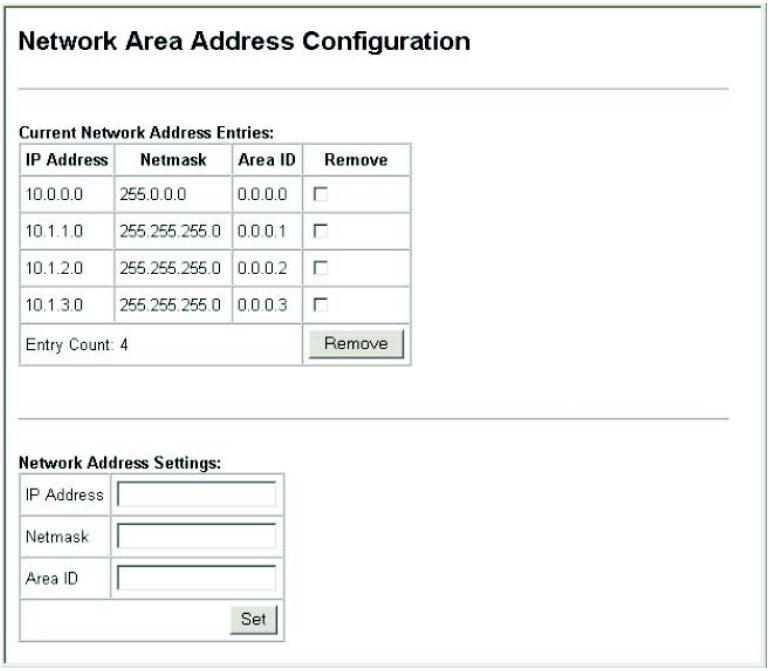


Figure 3-139 OSPF Network Area Address Configuration

CLI - This example configures the backbone area and one transit area.

```
Console(config-router)#network 10.0.0.0 255.0.0.0
  area 0.0.0.0                                                    4-348
Console(config-router)#network 10.1.1.0 255.255.255.0
  area 0.0.0.1
Console(config-router)#end
Console#show ip ospf                                              4-364
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 8 times
Area 0.0.0.1
     Number of interfaces in this area is 1
     SPF algorithm executed 5 times
Area 0.0.0.2 (STUB)
     Number of interfaces in this area is 1
     SPF algorithm executed 13 times
Area 0.0.0.3 (NSSA)
     Number of interfaces in this area is 1
     SPF algorithm executed 12 times
Console#
```

Configuring Summary Addresses (for External AS Routes)

An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols into all attached autonomous systems. (See "Redistributing External Routes" on page 3-327) To reduce the amount of external LSAs imported into your local routing domain, you can configure the router to advertise an aggregate route that consolidates a broad range of external addresses.

Command Usage

- If you are not sure what address ranges to consolidate, first enable external route redistribution via the Redistribute Configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.
- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 3-313).

Command Attributes

- **IP Address** – Summary address covering a range of addresses.
- **Netmask** – Network mask for the summary route.

Note: This router supports up 16 Type-5 summary routes.

Web - Click Routing Protocol, OSPF, Summary Address Configuration. Specify the base address and network mask, then click Add.

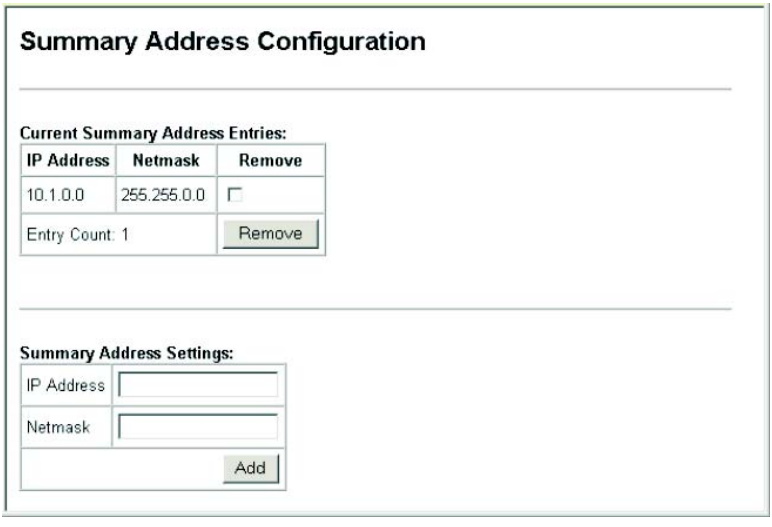


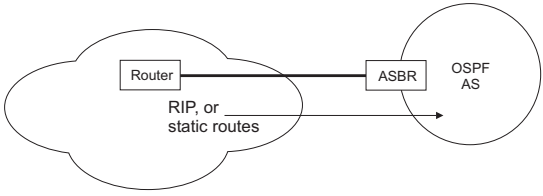
Figure 3-140 OSPF Summary Address Configuration

CLI - This example This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0
  255.255.0.0                                              4-346
Console(config-router)#
```

Redistributing External Routes

You can configure this router to import external routing information from other routing protocols into the autonomous system.



Command Usage

- This router supports redistribution for both RIP and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been manually configured as an ASBR via the General Configuration screen, but redistribution is not enabled, the router will only generate a "default" external route into the AS if it has been configured to "always" advertise a default route even if an external route does not actually exist (page 3-305).
- Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) via External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise external route metric.
- The metric value specified for redistributed routes supersedes the Default External Metric specified in the OSPF / General Configuration screen (page 3-305).

Command Attributes

- **Redistribute Protocol** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)
- **Redistribute Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)
- **Redistribute Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)

Web - Click Routing Protocol, OSPF, Redistribute. Specify the protocol type to import, the metric type and path cost, then click Add.

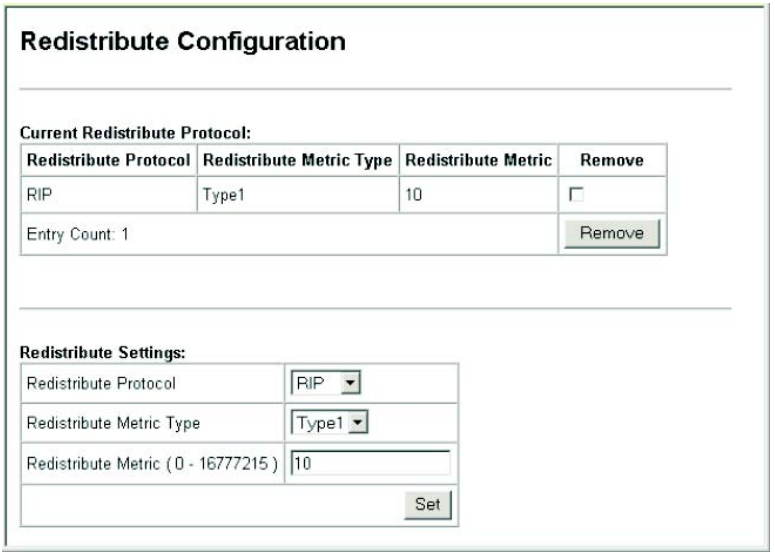


Figure 3-141 OSPF Redistribute Configuration

CLI - This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1          4-347
Console(config-router)#
```

Configuring NSSA Settings

Use the OSPF / NSSA Settings page to configure a not-so-stubby area (NSSA), and to control the use of default routes for ABRs and ASBRs, or external routes learned from other routing domains and imported via an ABR. (For a detailed description of NSSA areas, refer to "Configuring OSPF Areas" on page 3-309.)

Command Attributes

- **Area ID** – Identifier for an not-so-stubby area (NSSA).
- **Default Information Originate** – An NSSA ASBR originates and floods Type-7 external LSAs throughout its area for known network destination outside of the AS. However, you can also configure an NSSA ASBR to generate a Type-7 "default" route to areas outside of the AS, or an NSSA ABR to generate a Type-7 "default" route to other areas within the AS. (Default: Disabled)
- **No Redistribution** – The Redistribute Configuration page (page 3-327) is used to import information from other routing domains (or protocols) into the AS. However, when the router is an NSSA ABR, you can choose whether or not to accept external routes learned from routers in other OSPF areas into the NSSA. (Default: Enabled)

Note: This router supports up 16 areas, either normal transit areas, stubs, or NSSAs.

Web - Click Routing Protocol, OSPF, NSSA Settings. Create a new NSSA or modify the routing behavior for an existing NSSA, and click Apply.

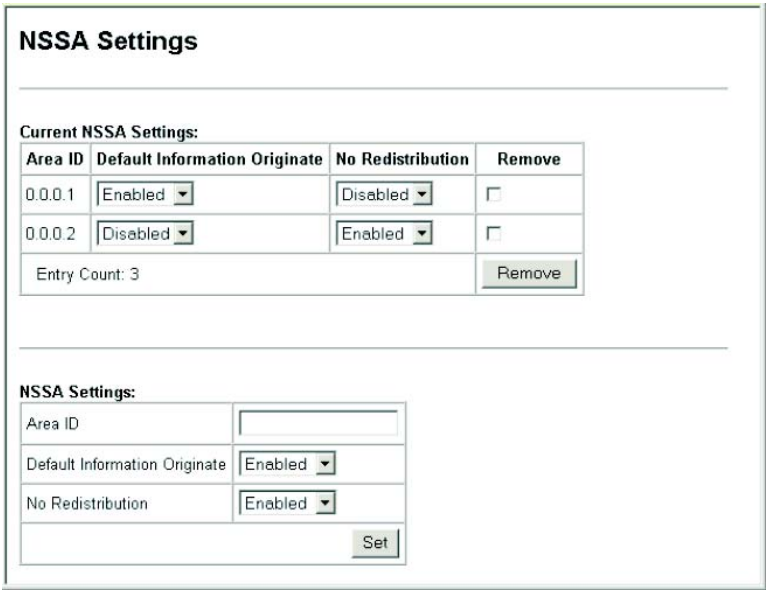


Figure 3-142 OSPF NSSA Settings

CLI - This example configures area 0.0.0.1 as a stub and sets the cost for the default summary route to 10.

```
Console(config-router)#area 0.0.0.1 nssa
  default-information- originate                                4-351
Console(config-router)#area 0.0.0.2 nssa no-redistribution     4-351
Console(config-router)#
```

Displaying Link State Database Information

OSPF routers advertise routes using Link State Advertisements (LSAs). The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. You can show information about different LSAs stored in this router's database, which may include any of the following types:

- Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.
- Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.
- Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.
- AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).
- AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.
- NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

Command Attributes

- **Area ID** – Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **Link ID** – The network portion described by an LSA. The Link ID should be:
  - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)
  - A Router ID for Router, Network, and Type 4 AS Summary LSAs.
- **Self-Originate** – Shows LSAs originated by this router.
- **LS Type** – LSA Type (Options: Type 1-5, 7). See the preceding description.

- **Adv Router** – IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- **Age**[25] – Age of LSA (in seconds).
- **Seq** – Sequence number of LSA (used to detect older duplicate LSAs).
- **CheckSum** – Checksum of the complete contents of the LSA.

Web - Click Routing Protocol, OSPF, Link State Database Information. Specify parameters for the LSAs you want to display, then click Query.

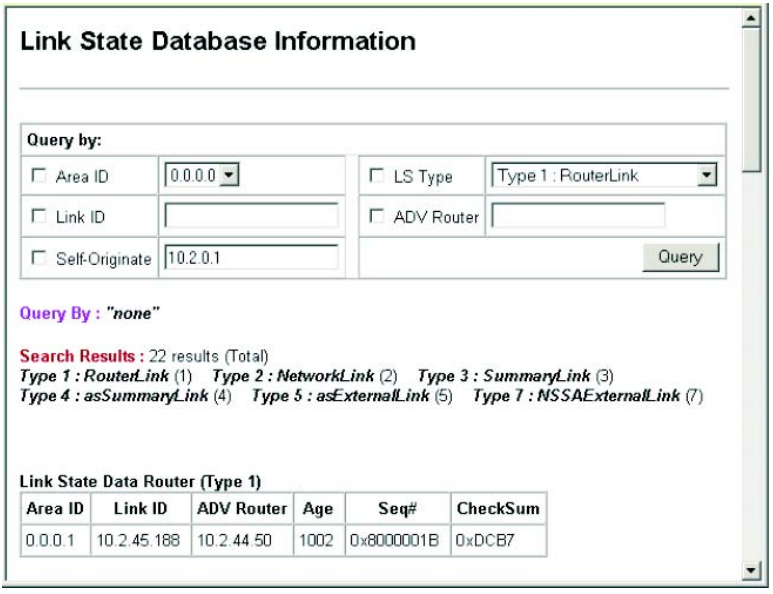


Figure 3-143 OSPF Link State Database Information

CLI - The CLI provides a wider selection of display options for viewing the Link State Database. See "show ip ospf database" on page -366.

25. These items are read only.

Displaying Information on Border Routers

You can display entries in the local routing table for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) known by this device.

Field Attributes

- **Destination** – Identifier for the destination router.
- **Next Hop** – IP address of the next hop toward the destination.
- **Cost** – Link metric for this route.
- **Type** – Router type of the destination; either ABR, ASBR or both.
- **Rte Type** – Route type; either intra-area or interarea route (INTRA or INTER).
- **Area** – The area from which this route was learned.
- **SPF No** – The number of times the shortest path first algorithm has been executed for this route.

Web - Click Routing Protocol, OSPF, Border Router Information.

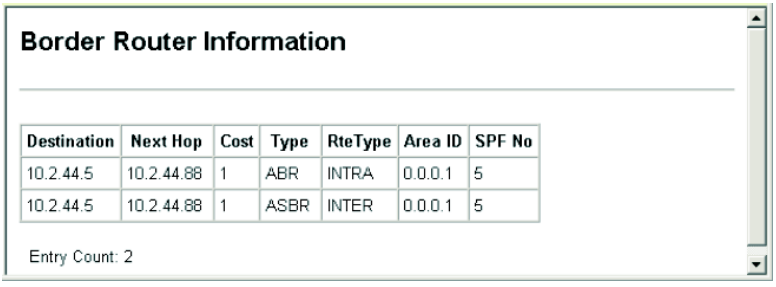


Figure 3-144 OSPF Border Router Information

CLI - This example shows one router that serves as both the ABR for the local area and the ASBR for the autonomous system.

```
Console#show ip ospf border-routers                                    4-365

  Destination      Next Hop      Cost   Type  RteType      Area         SPF No
------------- -------------- ------ ----- ------- -------------- -------
     10.2.44.5      10.2.44.88      1   ABR    INTRA          0.0.0.1       5
     10.2.44.5      10.2.44.88      1   ASBR   INTER          0.0.0.1       5
Console#
```

Displaying Information on Neighbor Routers

You can display about neighboring routers on each interface within an OSPF area.

Field Attributes

- **ID** – Neighbor's router ID.
- **Priority** – Neighbor's router priority.
- **State** – OSPF state and identification flag.

  States include:
  - Down – Connection down
  - Attempt – Connection down, but attempting contact (non-broadcast networks)
  - Init – Have received Hello packet, but communications not yet established
  - Two-way – Bidirectional communications established
  - ExStart – Initializing adjacency between neighbors
  - Exchange – Database descriptions being exchanged
  - Loading – LSA databases being exchanged
  - Full – Neighboring routers now fully adjacent

  Identification flags include:
  - D – Dynamic neighbor
  - S – Static neighbor
  - DR – Designated router
  - BDR – Backup designated router
- **Address** – IP address of this interface.

Web - Click Routing Protocol, OSPF, Neighbor Information.

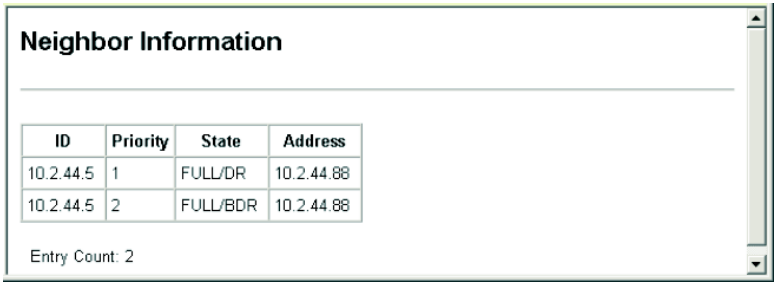


Figure 3-145 OSPF Neighbor Information

CLI - This shows a designated router and backup designated router as neighbors.

```
Console#show ip ospf neighbor                                    4-376

      ID          Pri         State          Address
--------------- ------ ---------------- ---------------
      10.2.44.5       1           FULL/DR       10.2.44.88
      10.2.44.6       2          FULL/BDR       10.2.44.88

Console#
```

CHAPTER 4
COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

Note: You can only access the console interface through the Master unit in the stack.

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the SMC8724ML3 L3 GE Switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is obtained via DHCP by default.

To access the stack through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the SMC8748ML3 L3 GE Switch is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "logging history" example, typing **log** followed by a tab will result in printing the command up to "**logging**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, DHCP, Interface, Line, Router, VLAN Database, or MSTP). You can also display a list of valid keywords for

a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  access-group        Access groups
  access-list         Access lists
  arp                 Information of ARP cache
  bridge-ext          Bridge extend information
  calendar            Date information
  class-map           Display class maps
  dns                 DNS information
  dot1x               Show 802.1x content
  garp                GARP property
  gvrp                Show GARP information of interface
  history             Information of history
  hosts               Host information
  interfaces          Information of interfaces
  ip                  IP information
  lacp                Show LACP statistic
  line                TTY line information
  logging             Show the contents of logging buffers
  mac                 MAC access lists
  mac-address-table   Set configuration of the address table
  management          Show management IP filter
  map                 Map priority
  marking             Specify marker
  policy-map          Display policy maps
  port                Characteristics of the port
  protocol-vlan       Protocol-VLAN information
  public-key          Show information of public key
  pvlan               Information of private VLAN
  queue               Information of priority queue
  radius-server       RADIUS server information
  rip                 RIP
  router              Router
  running-config      The system configuration of running
  snmp                SNMP statistics
  sntp                SNTP
  spanning-tree       Specify spanning-tree
  ssh                 Secure shell
  startup-config      The system configuration of starting up
  system              Information of system
  tacacs-server       Login by TACACS server
  users               Display information about terminal lines
  version             System hardware and software status
  vlan                Switch VLAN Virtual Interface
  vrrp                Show vrrp
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  counters       Information of interfaces counters
  protocol-vlan  Protocol-vlan information
  status         Information of interfaces status
  switchport     Information of interfaces switchport
Console#
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp            sntp            spanning-tree   ssh             standby
startup-config  system
Console#sh s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 4-1 General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List DHCP Interface Line Multiple Spanning Tree Router VLAN Database Class Map Policy Map

* You must be in Privileged Exec mode to access the Global configuration mode. You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password "admin." The system will now display the

"Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password "super" (page 4-37).

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

      CLI session with the SMC8748ML3 is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
 Username: guest
 Password: [guest login password]

       CLI session with the SMC8748ML3 is opened.
       To end the CLI session, enter [Exit].

 Console>enable
 Password: [privileged level password]
 Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- DHCP Configuration - These commands are used to configure the DHCP server.

- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Router Configuration - These commands configure global settings for unicast routing protocols.
- VLAN Configuration - Includes the command to create VLAN groups.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 4-2 Configuration Command Modes

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)#	4-14
Access Control List	access-list ip standard access-list ip extended access-list ip mask-precedence access-list mac access-list mac mask-precedence	Console(config-std-acl) Console(config-ext-acl) Console(config-ip-mask-acl) Console(config-mac-acl) Console(config-mac-mask-acl)	4-114
DHCP	ip dhcp pool	Console(config-dhcp)	4-157
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#	4-186
VLAN	vlan database	Console(config-vlan)	4-245
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	4-229
Router	router {rip | ospf}	Console(config-router)	4-325 4-340
Class Map	class map	Console(config-cmap)	4-286
Policy Map	policy map	Console(config-pmap)	4-289

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
:
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 4-3 Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Table 4-4 Command Group Index

Command Group	Description	Page
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out	4-14
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	4-26
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	4-32
Flash/File	Manages code image or switch configuration files	4-83
Authentication	Configures logon access using local or remote authentication; also configures port security and IEEE 802.1X port access control	4-91
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)	4-114
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	4-139
DHCP	Configures DHCP client, relay and server functions	4-157
DNS	Configures DNS services.	4-177
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	4-186
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	4-200
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	4-203
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	4-204

Table 4-4 Command Group Index (Continued)

Command Group	Description	Page
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	4-216
Spanning Tree	Configures Spanning Tree settings for the switch	4-221
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs and protocol VLANs	4-245
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for the bridge extension MIB	4-264
Priority	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	4-269
Quality of Service	Configures Differentiated Services	4-284
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	4-296
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters and static entries	4-307
IP Routing	Configures static and dynamic unicast routing	4-317
Router Redundancy	Configures router redundancy to create primary and backup routers	4-381

The access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
LC (Line Configuration)
IC (Interface Configuration)
VC (VLAN Database Configuration)
MST (Multiple Spanning Tree)
ACL (Access Control List Configuration)

DC (DHCP Server Configuration)
RC (Router Configuration)
CM (Class Map Configuration)
PM (Policy Map Configuration)

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 4-5 Line Commands

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	4-15
login	Enables password checking at login	LC	4-16
password	Specifies a password on a line	LC	4-17
timeout login response	Sets the interval that the system waits for a login attempt	LC	4-18
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	4-19
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	4-20
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	4-21
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	4-21
parity*	Defines the generation of a parity bit	LC	4-22
speed*	Sets the terminal baud rate	LC	4-23
stopbits*	Sets the number of the stop bits transmitted per byte	LC	4-24

Table 4-5 Line Commands (Continued)

Command	Function	Mode	Page
disconnect	Terminates a line connection	PE	4-24
show line	Displays a terminal line's parameters	NE, PE	4-25

* These commands only apply to the serial port.

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as "VTY" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (4-25)
show users (4-81)

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (4-35)
password (4-17)

password

This command specifies the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (4-16)
password-thresh (4-20)

timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

Syntax

timeout login response [*seconds*]
no timeout login response

seconds - Integer that specifies the timeout interval.
(Range: 0 - 300 seconds; 0: disabled)

Default Setting

- CLI: Disabled (0 seconds)
- Telnet: 600 seconds

Command Mode

Line Configuration

Command Usage

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]
no exec-timeout

seconds - Integer that specifies the timeout interval. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

- CLI: No timeout
- Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]
no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (4-21)

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (4-20)

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (4-22)

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default Setting

auto

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the "auto" option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier "0" will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

show ssh (4-55)
show users (4-81)

show line

This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout: Disabled
  Silent time:         Disabled
  Baudrate:            auto
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```

General Commands

Table 4-6 General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	4-27
disable	Returns to normal mode from privileged mode	PE	4-28
configure	Activates global configuration mode	PE	4-28
show history	Shows the command history buffer	NE, PE	4-29
reload	Restarts the system	PE	4-30
end	Returns to Privileged Exec mode	any config. mode	4-30
exit	Returns to the previous configuration mode, or exits the CLI	any	4-31
quit	Exits a CLI session	NE, PE	4-31
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 4-7.

Syntax

enable [*level*]

level - Privilege level to log into the device.
The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- "super" is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 4-37.)
- The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable (4-28)
enable password (4-37)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 4-7.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

enable (4-27)

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration. See "Understanding Command Modes" on page 4-7.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (4-30)

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

This command restarts the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

Table 4-7 System Management Commands

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	4-33
User Access	Configures the basic user names and passwords for management access	4-35
IP Filter	Configures IP addresses that are allowed management access	4-38
Web Server	Enables management access via a web browser	4-40
Telnet Server	Enables management access via Telnet	4-44
Secure Shell	Provides secure replacement for Telnet	4-45
Event Logging	Controls logging of error messages	4-57
SMTP Alerts	Configures SMTP email alerts	4-65
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually	4-69

Table 4-7 System Management Commands (Continued)

Command Group	Function	Page
System Status	Displays system configuration, active managers, and version information	4-75
Frame Size	Enables support for jumbo frames	4-82

Device Designation Commands

Table 4-8 Device Designation Commands

Command	Function	Mode	Page
prompt	Customizes the prompt used in PE and NE mode	GC	4-33
hostname	Specifies the host name for the switch	GC	4-34
snmp-server contact	Sets the system contact string	GC	4-142
snmp-server location	Sets the system location string	GC	4-143
switch renumber	Renumbers stack units	PE	4-34

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
```

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname RD#1
Console(config)#
```

switch renumber

This command resets the switch unit identification numbers in the stack. All stack members are numbered sequentially starting from the top unit for a non-loop stack, or starting from the Master unit for a looped stack.

Syntax

switch all renumber

Default Setting

- For non-loop stacking, the top unit is unit 1.
- For loop stacking, the master unit is unit 1.

Command Mode

Global Configuration

Example

This example shows how to renumber all units.

```
Console#switch all renumber
Console#
```

User Access Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 4-14), user authentication via a remote authentication server (page 4-91), and host access authentication for specific ports (page 4-104).

Table 4-9 User Access Commands

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	4-35
enable password	Sets a password to control access to the Privileged Exec level	GC	4-37

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** |
password {**0** | **7**} *password*}
no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
  The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.

- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

Table 4-10 Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.
  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is "super"

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 4-27).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (4-27)
authentication enable (4-93)

IP Filter Commands

Table 4-11 IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	4-38
show management	Displays the switch to be monitored or configured from a browser	PE	4-39

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- *start-address* - A single IP address, or the starting address of a range.
- *end-address* - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

Web Server Commands

Table 4-12 Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the web browser interface	GC	4-41
ip http server	Allows the switch to be monitored or configured from a browser	GC	4-41
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC	4-42
ip http secure-port	Specifies the UDP port number for HTTPS	GC	4-43

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (4-41)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[**no**] **ip http server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (4-41)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 6.2 or later versions.

- The following web browsers and operating systems currently support HTTPS:

Table 4-13 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 4-82. Also refer to the **copy** command on page 4-84.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (4-43)
copy tftp https-certificate (4-84)

ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device*:*port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (4-42)

Telnet Server Commands

Table 4-14 Telnet Server Commands

Command	Function	Mode	Page
ip telnet server	Allows the switch to be monitored or configured from Telnet; also specifies the port to be used by the Telnet interface	GC	4-41

ip telnet server

This command allows this device to be monitored or configured from Telnet. It also specifies the TCP port number used by the Telnet interface. Use the **no** form without the "port" keyword to disable this function. Use the **no** from with the "port" keyword to use the default port.

Syntax

ip telnet server [**port** *port-number*]
no telnet server [**port**]

- **port** - The TCP port number used by the Telnet interface.
- *port-number* - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

- Server: Enabled
- Server Port: 23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#ip telnet port 123
Console(config)#
```

Secure Shell Commands

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When a client contacts the switch via the SSH protocol, the switch uses a public-key that the client must match along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

This section describes the commands used to configure the SSH server. However, note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 4-15 Secure Shell Commands

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	4-48
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	4-49
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	4-50
ip ssh server-key size	Sets the SSH server key size	GC	4-51
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE	4-84
delete public-key	Deletes the public key for the specified user	PE	4-51
ip ssh crypto host-key generate	Generates the host key	PE	4-52
ip ssh crypto zeroize	Clear the host key from RAM	PE	4-53
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	4-54
disconnect	Terminates a line connection	PE	4-24
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	4-54
show ssh	Displays the status of current SSH sessions	PE	4-55
show public-key	Shows the public key for the specified user or for the host	PE	4-56
show users	Shows SSH users, including privilege level and public key type	PE	4-81

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 4-92. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the

switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.
2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:
   10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167097480477611 7
3. Import Client's Public Key to the Switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the **username** command as described on page 4-35.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:
   1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19
4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the switch.

6. Configure Challenge-Response Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can gain access. The following exchanges take place during this process:

   a. The client sends its public key to the switch.
   b. The switch compares the client's public key to those stored in memory.
   c. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
   d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.
   e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

[**no**] **ip ssh server**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate DSA and RSA host keys before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (4-52)
show ssh (4-55)

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (4-19)
show ip ssh (4-54)

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (4-54)

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*
no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

- The server key is a private key that is never shared outside the switch.
- The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

This command deletes the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

- *username* – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** – DSA (Version 2) key type.
- **rsa** – RSA (Version 1) key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- This command stores the host key pair in memory (i.e., RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

ip ssh crypto zeroize (4-53)
ip ssh save host-key (4-54)

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (4-52)
ip ssh save host-key (4-54)
no ip ssh server (4-48)

ip ssh save host-key

This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (4-52)

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show ssh

This command displays the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5
Console#
```

Table 4-16 show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5

Table 4-16 show ssh - display description (Continued)

Field	Description
	Terminology: DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

show public-key

This command shows the public key for the specified user or for the host.

Syntax

show public-key [**user** [*username*] | **host**]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 65537
   13236940658254764031382795526536375927835525327972629521130241
   07194210616557594245909392360969540503627752575562510038661309893 93
   83452310332802149888661921595568598879891919505883940181387440468 90
   87791603058377681854900028313416250083487184495220874292122556916 65
   65529632816351696404083155476606641516570116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h
   2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFf
   AKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAA
   FQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+
   /p9cnrfwFTMU01VFDly3IR 2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNO
   xrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2
   eTCD5nekAAACBAJ8rMccXTxHLFAczWS7Ej0y DbsloBfPuSAb4oAsyjKXKVYNLQkTLZ
   fcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2o/dVzX4Gg+yqdTlYmGA7fHGm
   8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7 w0W
Console#
```

Event Logging Commands

Table 4-17 Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	4-58
logging history	Limits syslog messages saved to switch memory based on severity	GC	4-58
logging host	Adds a syslog server host IP address that will receive logging messages	GC	4-60
logging facility	Sets the facility type for remote logging of syslog messages	GC	4-60
logging trap	Limits syslog messages saved to a remote server based on severity	GC	4-61
clear log	Clears messages from the logging buffer	PE	4-62
show logging	Displays the state of logging	PE	4-62
show log	Displays log messages	PE	4-64

logging on

This command controls logging of error messages, sending debug or error messages to switch memory. The **no** form disables the logging process.

Syntax

[**no**] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory. You can use the **logging history** command to control the type of error messages that are stored.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (4-58)
clear log (4-62)

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).

- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 4-18 Logging Levels

Level	Severity Name	Description
7	debugging	Debugging messages
6	informational	Informational messages only
5	notifications	Normal but significant condition, such as cold start
4	warnings	Warning conditions (e.g., return false, unexpected return)
3	errors	Error conditions (e.g., invalid input, default used)
2	critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	alerts	Immediate action needed
0	emergencies	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

- Flash: errors (level 3 - 0)
- RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

[**no**] **logging host** *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

[**no**] **logging facility** *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

Syntax

logging trap [*level*]
no logging trap

level - One of the syslog severity levels listed in the table on page 4-58. Messages sent include the selected level up through level 0.

Default Setting

- Disabled
- Level 7 - 0

Command Mode

Global Configuration

Command Usage

- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear log

This command clears messages from the log buffer.

Syntax

clear log [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear log
Console#
```

Related Commands

show log (4-64)

show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

show logging {**flash** | **ram** | **sendmail** | **trap**}

- **flash** - Displays settings for storing event messages in flash memory (i.e., permanent memory).
- **ram** - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

- **sendmail** - Displays settings for the SMTP event handler (page 4-69).
- **trap** - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), and the message level for RAM is "debugging" (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
Console#
```

Table 4-19 show logging flash/ram - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
History logging in FLASH	The message level(s) reported based on the **logging history** command.
History logging in RAM	The message level(s) reported based on the **logging history** command.

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type:        Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

Table 4-20 show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
REMOTELOG status	Shows if remote logging has been enabled via the **logging trap** command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the **logging facility** command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the **logging trap** command.
REMOTELOG server IP address	The address of syslog servers as specified in the **logging host** command.

Related Commands

show logging sendmail (4-69)

show log

This command displays the log messages stored in local memory.

Syntax

show log {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

SMTP Alert Commands

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 4-21 SMTP Alert Commands

Command	Function	Mode	Page
logging sendmail host	SMTP servers to receive alert messages	GC	4-65
logging sendmail level	Severity threshold used to trigger alert messages	GC	4-66
logging sendmail source-email	Email address used for "From" field of alert messages	GC	4-67
logging sendmail destination-email	Email recipients of alert messages	GC	4-68
logging sendmail	Enables SMTP event handling	GC	4-68
show logging sendmail	Displays SMTP event handler settings	NE, PE	4-69

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[**no**] **logging sendmail host** *ip_address*

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level *level*

level - One of the system message levels (page 4-58). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the "From" field in alert messages.

Syntax

logging sendmail source-email *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email
   ted@this-company.com
Console(config)#
```

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[**no**] **logging sendmail**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
------------------------------------------------
192.168.1.19

SMTP minimum severity level: 7

SMTP destination email addresses
------------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enabled
Console#
```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 4-22 Time Commands

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	4-70
sntp server	Specifies one or more time servers	GC	4-71
sntp poll	Sets the interval at which the client polls for time	GC	4-72

Table 4-22 Time Commands (Continued)

Command	Function	Mode	Page
show sntp	Shows current SNTP configuration settings	NE, PE	4-73
clock timezone	Sets the time zone for the switch's internal clock	GC	4-73
calendar set	Sets the system date and time	PE	4-74
show calendar	Displays the current date and time setting	NE, PE	4-75

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form to disable SNTP client requests.

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

Related Commands

sntp server (4-71)
sntp poll (4-72)
show sntp (4-73)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (4-70)
sntp poll (4-72)
show sntp (4-73)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*
no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (4-70)

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 0-13 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (4-73)

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit). (Range: 2001 - 2100)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar
 15:12:34 February 1 2002
Console#
```

System Status Commands

Table 4-23 System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	4-76
show running-config	Displays the configuration data currently in use	PE	4-78
show system	Displays system information	NE, PE	4-80
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	4-81
show version	Displays version information for the system	NE, PE	4-81

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for each switch in the stack
  - SNTP server settings
  - SNMP community strings
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-20-1a-df-9e-c0_01</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
phymap 00-20-1a-df-9e-c0 00-00-00-00-00-00 00-00-00-00-00-00
   00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
   00-00-00-00-00-00 00-00-00-00-00-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community public ro
snmp-server community private rw
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree MST configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 queue bandwidth 0 0 0 0 0 0 0 0
:
interface VLAN 1
 ip address DHCP
!
no map IP precedence
no map IP DSCP
!
line console
!
line vty
!
end
!
Console#
```

Related Commands

show running-config (4-78)

show running-config

This command displays the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for each switch in the stack
  - SNTP server settings
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-30-f1-d4-73-a0_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
phymap 00-30-f1-d4-73-a0 00-00-00-00-00-00 00-00-00-00-00-00
   00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
   00-00-00-00-00-00 00-00-00-00-00-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree MST-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
:
interface VLAN 1
 IP address DHCP
!
no map IP precedence
no map IP DSCP
!
line console
line vty
!
end
Console#
```

Related Commands

show startup-config (4-76)

show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to "Displaying System Information" on page 3-15.
- The POST results should all display "PASS." If any POST test indicates "FAIL," contact your distributor for assistance.

Example

```
Console#show system
System description: SMC8748ML3 L3 GE Switch
System OID string: 1.3.6.1.4.1.202.20.45
System information
 System Up time:          0 days, 0 hours, 11 minutes, and 15.59
   seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC address (unit1):   00-20-1A-DF-9E-C0
 Web server:              enabled
 Web server port:         80
 Web secure server:       enabled
 Web secure server port:  443
 Telnet server:           enable
 Telnet server port:      23
 Jumbo Frame:             Disabled
 POST result
DUMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
Timer Test ................... PASS
PCI Device 1 Test ............ PASS
I2C Bus Initialization ....... PASS
Switch Int Loopback Test ..... PASS
Crossbar Int Loopback Test ... PASS
Fan Speed Test ............... PASS

Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None
     steve        15        RSA

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:14:14
* 1     VTY 0    admin           0:00:00    192.168.1.19
  2     SSH 1    steve           0:00:06    192.168.1.19

 Web online users:
  Line        Remote IP addr Username Idle time (h:m:s).
  ----------- -------------- -------- ------------------
 1      HTTP   192.168.1.19    admin           0:00:00

Console#
```

show version

This command displays hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See "Displaying Switch Hardware/Software Versions" on page 3-17 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit1
 Serial number:            A422000632
 Hardware version:         R01
 EPLD version:             15.15
 Number of ports:          24
 Main power status:        up
 Redundant power status:   not present

Agent (master)
 Unit ID:                  1
 Loader version:           1.0.1.3
 Boot ROM version:         1.0.1.6
 Operation code version:   1.0.0.0

Console#
```

Frame Size Commands

Table 4-24 Frame Size Commands

Command	Function	Mode	Page
jumbo frame	Enables support for jumbo frames	GC	4-82

jumbo frame

This command enables support for jumbo frames. Use the **no** form to disable it.

Syntax

[no] jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- The current setting for jumbo frames can be displayed with the **show system** command (page 4-80).

Example

```
Console(config)#jumbo frame
Console(config)#
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Table 4-25 Flash/File Commands

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	4-84
delete	Deletes a file or code image	PE	4-87
dir	Displays a list of files in flash memory	PE	4-88
whichboot	Displays the files booted	PE	4-89
boot system	Specifies the file or image used to start up the system	GC	4-90

copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp | unit**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** | **https-certificate | public-key**}
copy unit file

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Keyword that allows you to copy the HTTPS secure site certificate.
- **public-key** - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell Commands" on page 4-45.)
- **unit** - Keyword that allows you to copy to/from a specific unit in the stack.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length

for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- Use the **copy file** unit command to copy a local file to another switch in the stack. Use the **copy unit file** command to copy a file from another switch in the stack.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" on page 3-82. For information on configuring the switch to use HTTPS for a secure connection, see "ip http secure-server" on page 4-42.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

delete

This command deletes a file or image.

Syntax

delete [*unit*:] *filename*

- *filename* - Name of configuration file or code image.
- *unit* - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- "Factory_Default_Config.cfg" cannot be deleted.
- A colon (:) is required after the specified unit number.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (4-88)
delete public-key (4-51)

dir

This command displays a list of files in flash memory.

Syntax

dir [*unit***:**] {{**boot-rom:** | **config:** | **opcode:**} [*filename*]}

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.
- *unit* - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- A colon (:) is required after the specified unit number.
- File information is shown below:

Table 4-26 File Directory Information

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
          file name                          file type       startup size (byte)
 ------------------------------------     --------------  ------- -----------
 Unit1:
          D1016                              Boot-Rom image  Y           825500
          V1000                              Operation Code  Y          3511280
          Factory_Default_Config.cfg         Config File     N              455
          startup                            Config File     Y             4308
          startup1.cfg                       Config File     N             4268
 ------------------------------------------------------------------------------
                                                    Total free space:  24117248
Console#
```

whichboot

This command displays which files were booted when the system powered up.

Syntax

whichboot [*unit*]

unit - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
                       file name                file type startup size (byte)
 ------------------------------- ----------------------- ------- -----------
 Unit1:
          D1016                              Boot-Rom image  Y           825500
          V1000                              Operation Code  Y          3511280
          startup                            Config File     Y             4308
Console#
```

boot system

This command specifies the file or image used to start up the system.

Syntax

boot system [*unit*:] {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom*** - Boot ROM.
- **config*** - Configuration file.
- **opcode*** - Run-time operation code.
- *filename* - Name of configuration file or code image.
- *unit** - Stack unit. (Range: 1-8)

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified unit number and file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (4-88)
whichboot (4-89)

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1X.

Table 4-27 Authentication Commands

Command Group	Function	Page
Authentication Sequence	Defines logon authentication method and precedence	4-91
RADIUS Client	Configures settings for authentication via a RADIUS server	4-94
TACACS+ Client	Configures settings for authentication via a TACACS+ server	4-99
Port Security	Configures secure addresses for a port	4-101
Port Authentication	Configures host authentication on specific ports using 802.1X	4-104

Authentication Sequence

Table 4-28 Authentication Sequence Commands

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	4-92
authentication enable	Defines the authentication method and precedence for command mode change	GC	4-93

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local password.
- **radius** - Use RADIUS server password.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (4-35)

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command (see page 4-27). Use the **no** form to restore the default.

Syntax

authentication enable {[**local**] [**radius**] [**tacacs**]}
no authentication enable

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+

server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

enable password - sets the password for changing command modes (4-37)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 4-29 RADIUS Client Commands

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	4-95
radius-server port	Sets the RADIUS server network port	GC	4-96
radius-server key	Sets the RADIUS encryption key	GC	4-96
radius-server retransmit	Sets the number of retries	GC	4-97
radius-server timeout	Sets the interval between sending authentication requests	GC	4-97
show radius-server	Shows the current RADIUS settings	PE	4-98

radius-server host

This command specifies primary and backup RADIUS servers and authentication parameters that apply to each server. Use the **no** form to restore the default values.

Syntax

[**no**] **radius-server** *index* **host** {*host_ip_address* | *host_alias*}
[**auth-port** *auth_port*] [**timeout** *timeout*] [**retransmit** *retransmit*] [**key** *key*]

- *index* - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.
- *host_ip_address* - IP address of server.
- *host_alias* - Symbolic name of server. (Maximum length: 20 characters)
- *port_number* - RADIUS serverUDP port used for authentication messages. (Range: 1-65535)
- *timeout* - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)
- *retransmit* - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)
- *key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

- **auth-port** - 1812
- **timeout** - 5 seconds
- **retransmit** - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
  retransmit 5 key green
Console(config)#
```

radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   1812
 Retransmit times:                     2
 Request timeout:                      5

Server 1:
 Server IP address:                    192.168.1.1
 Communication key with RADIUS server: *****
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5

Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 4-30 TACACS+ Client Commands

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	4-99
tacacs-server port	Specifies the TACACS+ server network port	GC	4-100
tacacs-server key	Sets the TACACS+ encryption key	GC	4-100
show tacacs-server	Shows the current TACACS+ settings	GC	4-101

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address:                    10.11.12.13
 Communication key with TACACS server: *****
 Server port number:                   49
Console#
```

Port Security Commands

These commands can be used to enable port security on a port. When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 4-31 Port Security Commands

Command	Function	Mode	Page
port security	Configures a secure port	IC	4-102
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-217
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-219

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]
no port security [**action** | **max-mac-count**]

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable port.
- **max-mac-count**
  - *address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

- Status: Disabled
- Action: None
- Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum

number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port.
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- You can also manually add secure addresses with the **mac-address-table static** command.
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN port.
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown (4-193)
mac-address-table static (4-217)
show mac-address-table (4-219)

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 4-32 802.1X Port Authentication Commands

Command	Function	Mode	Page
dot1x system-auth-control	Enables dot1x globally on the switch.	GC	4-105
dot1x default	Resets all dot1x parameters to their default values	GC	4-105
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/ identity packet to the client before it times out the authentication session	IC	4-105
dot1x port-control	Sets dot1x mode for a port interface	IC	4-106
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC	4-107
dot1x re-authenticate	Forces re-authentication on specific ports	PE	4-108
dot1x re-authentication	Enables re-authentication for all ports	IC	4-108
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC	4-109
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC	4-109
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC	4-110
show dot1x	Shows all dot1x related information	PE	4-110

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[**no**] **dot1x system-auth-control**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control
Console(config)#
```

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*]}
no dot1x operation-mode [**multi-host max-count**]

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple host to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
  count – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- The "max-count" parameter specified by this command is only effective if the dot1x mode is set to "auto" by the dot1x port-control command (page 4-105).
- In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

[**no**] **dot1x re-authentication**

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*
no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

- **statistics** - Displays dot1x status for each port.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch.
- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
  - Status – Administrative state for port access control.
  - Operation Mode – Allows single or multiple hosts (page 4-107).
  - Mode – Dot1x port control mode (page 4-106).
  - Authorized – Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
  - reauth-enabled – Periodic re-authentication (page 4-108).
  - reauth-period – Time after which a connected client must be re-authenticated (page 4-109).
  - quiet-period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 4-109).
  - tx-period – Time a port waits during authentication session before re-transmitting EAP packet (page 4-110).
  - supplicant-timeout– Supplicant timeout.
  - server-timeout – Server timeout.
  - reauth-max – Maximum number of reauthentication attempts.
  - max-req – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 4-105).
  - Status – Authorization status (authorized or not).
  - Operation Mode – Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.

- Max Count – The maximum number of hosts allowed to access this port (page 4-107).
- Port-control – Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 4-106).
- Supplicant – MAC address of authorized client.
- Current Identifier – The integer (0-255) used by the Authenticator to identify the current authentication session.

• *Authenticator State Machine*
- State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- Reauth Count – Number of times connecting state is re-entered.

• *Backend State Machine*
- State – Current state (including request, response, success, fail, timeout, idle, initialize).
- Request Count – Number of EAP Request packets sent to the Supplicant without receiving a response.
- Identifier(Server) – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

• *Reauthentication State Machine*
- State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode              Authorized
1/1        disabled       Single-Host      ForceAuthorized     n/a
1/2        disabled       Single-Host      ForceAuthorized     n/a
:
1/23       disabled       Single-Host      ForceAuthorized     yes
1/24       enabled        Single-Host      Auto                yes


802.1X Port Details

802.1X is enabled on port 1/1
:

802.1X is enabled on port 26
reauth-enabled:       Enable
reauth-period:        3600
quiet-period:         60
tx-period:            30
supplicant-timeout:   30
server-timeout:       10
reauth-max:           2
max-req:              2
Status                Authorized
Operation mode        Multi-Host
Max count             5
Port-control          Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    3

Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize

Console#
```

Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

The following restrictions apply to ACLs:

- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress

filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.

- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.
- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Masks for Access Control Lists

You must specify masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny the rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ACL. A mask must

be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Table 4-33 Access Control List Commands

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	4-116
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	4-128
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	4-137

IP ACLs

Table 4-34 IP ACL Commands

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IP ACLs	GC	4-117
permit, deny	Filters packets matching a specified source IP address	STD-ACL	4-118
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	4-119
show ip access-list	Displays the rules for configured IP ACLs	PE	4-121
access-list ip mask-precedence	Changes to the IP Mask mode used to configure access control masks	GC	4-122
mask	Sets a precedence mask for the ACL rules	IP-Mask	4-123
show access-list ip mask-precedence	Shows the ingress or egress rule masks for IP ACLs	PE	4-126
ip access-group	Adds a port to an IP ACL	IC	4-127
show ip access-group	Shows port assignments for IP ACLs	PE	4-127

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ip** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny 4-118
ip access-group (4-127)
show ip access-list (4-121)

permit, deny (Standard ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} {**any** | *source bitmask* | **host** *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (4-117)

permit, deny (Extended ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]

[**no**] {**permit | deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- *precedence* – IP precedence level. (Range: 0-7)
- *tos* – Type of Service level. (Range: 0-15)
- *dscp* – DSCP priority level. (Range: 0-63)
- *sport* – Protocol[26] source port number. (Range: 0-65535)
- *dport* – Protocol[26] destination port number. (Range: 0-65535)
- *port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)
- *control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *flag-bitmask* – Decimal number representing the code bits to match.

26. Includes TCP, UDP or other protocol types.

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use "control-code 2 2"
  - Both SYN and ACK valid, use "control-code 18 18"
  - SYN valid and ACK invalid, use "control-code 2 18"

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
  destination-port 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-ext-acl)#
```

Related Commands

access-list ip (4-117)

show ip access-list

This command displays the rules for configured IP ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands

permit, deny 4-118
ip access-group (4-127)

access-list ip mask-precedence

This command changes to the IP Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified IP ACLs.

Command Mode

Global Configuration

Command Usage

- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Example

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#
```

Related Commands

mask (IP ACL) (4-123)
ip access-group (4-127)

mask (IP ACL)

This command defines a mask for IP ACLs. This mask defines the fields to check in the IP header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**protocol**]
{**any** | **host** | *source-bitmask*}
{**any** | **host** | *destination-bitmask*}
[**precedence**] [**tos**] [**dscp**]
[**source-port** [*port-bitmask*]] [**destination-port** [*port-bitmask*]]
[**control-flag** [*flag-bitmask*]]

- **protocol** – Check the protocol field.
- **any** – Any address will be matched.
- **host** – The address must be for a host device, not a subnetwork.
- *source-bitmask* – Source address of rule must match this bitmask.
- *destination-bitmask* – Destination address of rule must match this bitmask.
- **precedence** – Check the IP precedence field.
- **tos** – Check the TOS field.
- **dscp** – Check the DSCP field.
- **source-port** – Check the protocol source port field.
- **destination-port** – Check the protocol destination port field.
- *port-bitmask* – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **control-flag** – Check the field for control flags.
- *flag-bitmask* – Control flags of rule must match this bitmask. (Range: 0-63)

Default Setting

None

Command Mode

IP Mask

Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and ingress or egress masks before mapping an ACL to an interface.
- If you enter **dscp**, you cannot enter **tos** or **precedence**. You can enter both **tos** and **precedence** without **dscp**.
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Example

This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the "deny 10.1.1.1 255.255.255.255" rule has the higher precedence according the "mask host any" entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit any
Console(config-std-acl)#deny host 171.69.198.102
Console(config-std-acl)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A2 in
Console(config-if)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#
```

This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23.

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any
   source-port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
  deny host 171.69.198.5 any
  deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
  deny 171.69.198.0 255.255.255.0 any source-port 23
  deny host 171.69.198.5 any
IP egress mask ACL:
  mask 255.255.255.0 any source-port
Console#
```

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL. Note that once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

```
Switch(config)#access-list ip extended 6
Switch(config-ext-acl)#permit any any
Switch(config-ext-acl)#deny tcp any any control-flag 2 2
Switch(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
Console#configure
Switch(config)#access-list ip mask-precedence in
Switch(config-ip-mask-acl)#mask protocol any any control-flag 2
Switch(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-list ip mask-precedence

This command shows the ingress or egress rule masks for IP ACLs.

Syntax

show access-list ip mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

```
Console#show access-list ip mask-precedence
IP ingress mask ACL:
  mask host any
  mask 255.255.255.0 any
Console#
```

Related Commands

mask (IP ACL) (4-123)

ip access-group

This command binds a port to an IP ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ip access-group** *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (4-121)

show ip access-group

This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
 IP standard access-list david
Console#
```

Related Commands

ip access-group (4-127)

MAC ACLs

Table 4-35 MAC ACL Commands

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	4-129
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL	4-130
show mac access-list	Displays the rules for configured MAC ACLs	PE	4-132
access-list mac mask-precedence	Changes to the mode for configuring access control masks	GC	4-132
mask	Sets a precedence mask for the ACL rules	MAC-Mask	4-133
show access-list mac mask-precedence	Shows the ingress or egress rule masks for MAC ACLs	PE	4-135
mac access-group	Adds a port to a MAC ACL	IC	4-136
show mac access-group	Shows port assignments for MAC ACLs	PE	4-137

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list mac** *acl_name*

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny (4-130)
mac access-group (4-136)
show mac access-list (4-132)

permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

Note:- The default is for Ethernet II packets.

[**no**] {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

- **tagged-eth2** – Tagged Ethernet II packets.
- **untagged-eth2** – Untagged Ethernet II packets.
- **tagged-802.3** – Tagged Ethernet 802.3 packets.
- **untagged-802.3** – Untagged Ethernet 802.3 packets.
- **any** – Any MAC source or destination address.
- **host** – A specific MAC address.
- *source* – Source MAC address.

- *destination* – Destination MAC address range with bitmask.
- *address-bitmask*[27] – Bitmask for MAC address (in hexidecimal format).
- vid – VLAN ID. (Range: 1-4093)
- *vid-bitmask*[27] – VLAN bitmask. (Range: 1-4093)
- *protocol* – A specific Ethernet protocol number. (Range: 600-fff hex.)
- *protocol-bitmask*[27] – Protocol bitmask. (Range: 600-fff hex.)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
   ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (4-129)

27. For all bitmasks, "1" means care and "0" means ignore.

show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl_name*]

acl_name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny 4-130
mac access-group (4-136)

access-list mac mask-precedence

This command changes to MAC Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified MAC ACLs.

Command Mode

Global Configuration

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.

Example

```
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#
```

Related Commands

mask (MAC ACL) (4-133)
mac access-group (4-136)

mask (MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**pktformat**]
{**any** | **host** | *source-bitmask*} {**any** | **host** | *destination-bitmask*}
[**vid** [*vid-bitmask*]] [**ethertype** [*ethertype-bitmask*]]

- **pktformat** – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- **any** – Any address will be matched.
- **host** – The address must be for a single node.
- *source-bitmask* – Source address of rule must match this bitmask.
- *destination-bitmask* – Destination address of rule must match this bitmask.
- **vid** – Check the VLAN ID field.
- *vid-bitmask* – VLAN ID of rule must match this bitmask.

- **ethertype** – Check the Ethernet type field.
- *ethertype-bitmask* – Ethernet type of rule must match this bitmask.

Default Setting

None

Command Mode

MAC Mask

Command Usage

- Up to seven masks can be assigned to an ingress or egress ACL.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

Example

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
  ff-ff-ff-ff-ff-ff any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
   permit any any
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
   permit any any
MAC ingress mask ACL:
   mask pktformat host any vid
Console#
```

This example creates an Egress MAC ACL.

```
Console(config)#access-list mac M5
Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
  ff-ff-ff-ff-ff-ff any vid 3 ethertype 0806
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M5:
   deny tagged-802.3 host 00-11-11-11-11-11 any
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
Console(config)#access-list mac mask-precedence out
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#mac access-group M5 out
Console(config-if)#end
Console#show access-list
MAC access-list M5:
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
   deny tagged-802.3 host 00-11-11-11-11-11 any
MAC ingress mask ACL:
   mask pktformat host any vid ethertype
Console#
```

show access-list mac mask-precedence

This command shows the ingress or egress rule masks for MAC ACLs.

Syntax

show access-list mac mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

```
Console#show access-list mac mask-precedence
MAC egress mask ACL:
   mask pktformat host any vid ethertype
Console#
```

Related Commands

mask (MAC ACL) (4-133)

mac access-group

This command binds a port to a MAC ACL. Use the **no** form to remove the port.

Syntax

mac access-group *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (4-132)

show mac access-group

This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 out
Console#
```

Related Commands

mac access-group (4-136)

ACL Information

Table 4-36 ACL Information Commands

Command	Function	Mode	Page
show access-list	Show all ACLs and associated rules	PE	4-137
show access-group	Shows the ACLs assigned to each port	PE	4-138

show access-list

This command shows all ACLs and associated rules, as well as all the user-defined masks.

Command Mode

Privileged Exec

Command Usage

Once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-group

This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
 IP standard access-list david
 MAC access-list jerry
Console#
```

SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 4-37 SNMP Commands

Command	Function	Mode	Page
snmp-server	Enables the SNMP agent	GC	4-140
show snmp	Displays the status of SNMP communications	NE, PE	4-140
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	4-141
snmp-server contact	Sets the system contact string	GC	4-142
snmp-server location	Sets the system location string	GC	4-143
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	4-143
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	4-146
snmp-server engine-id	Sets the SNMP engine ID	GC	4-147
show snmp engine-id	Shows the SNMP engine ID	PE	4-149
snmp-server view	Adds an SNMP view	GC	4-150
show snmp view	Shows the SNMP views	PE	4-151
snmp-server group	Adds an SNMP group, mapping users to views	GC	4-152

Table 4-37 SNMP Commands (Continued)

Command	Function	Mode	Page
show snmp group	Shows the SNMP groups	PE	4-153
snmp-server user	Adds a user to an SNMP group	GC	4-154
show snmp user	Shows the SNMP users	PE	4-156

snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[no] snmp-server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

show snmp

This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP Agent: enabled

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```

snmp-server community

This command defines the SNMP v1 and v2c community access string. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (4-143)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (4-142)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]] *community-string* [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}
no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)

- **inform** - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - *retries* - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
  - *seconds* - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- *community-string* - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)
  - **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 3-50 for further information about these authentication and encryption options.
- *port* - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

- Host Address: None
- Notification Type: Traps
- SNMP Version: 1
- UDP Port: 162

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable

multiple hosts, you must issue a separate **snmp-server host** command for each host.

- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 4-140).
  2. Allow the switch to send SNMP traps; i.e., notifications (page 4-146).
  3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
  4. Create a view with the required notification messages (page 4-150).
  5. Create a group that includes the required notify view (page 4-152).

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 4-140).
  2. Allow the switch to send SNMP traps; i.e., notifications (page 4-146).
  3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
  4. Create a view with the required notification messages (page 4-150).
  5. Create a group that includes the required notify view (page 4-152).
  6. Specify a remote engine ID where the user resides (page 4-147).

7. Then configure a remote user (page 4-154).

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. If you use the V3 "auth" or "priv" options, the user name must first be defined with the **snmp-server user** command. Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the "noauth" option, an SNMP user account will be generated, and the switch will authorize SNMP access for the host.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (4-146)

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure notifications.
- **link-up-down** - Keyword to issue link-up or link-down notifications.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command (page 4-152).

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (4-143)

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*
no snmp-server engine-id {**local** | **remote** {**address**}}

- **local** - Specifies the SNMP engine on this switch.
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- *engineid-string* - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See **snmp-server host** on page 4-143..) The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.
- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "1234" is equivalent to "1234" followed by 22 zeroes.
- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 4-154).

Example

```
Console(config)#snmp-server engine-id local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#
```

Related Commands

snmp-server host (4-143)

show snmp engine-id

This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                        IP address
80000000030004e2b316c54321                                  192.168.1.19
Console#
```

Table 4-38 show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

- *view-name* - Name of an SNMP view. (Range: 1-64 characters)
- *oid-tree* - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)
- **included** - Defines an included view.
- **excluded** - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- Views are used in the **snmp-server group** command to restrict user access to specified portions of the MIB tree.
- The predefined view "defaultview" includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
   included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
   included
Console(config)#
```

show snmp view

This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

Console#
```

Table 4-39 show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

no snmp-server group *groupname*

- *groupname* - Name of an SNMP group. (Range: 1-32 characters)
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 3-50 for further information about these authentication and encryption options.
- *readview* - Defines the view for read access. (1-64 characters)
- *writeview* - Defines the view for write access. (1-64 characters)
- *notifyview* - Defines the view for notifications. (1-64 characters)

Default Setting

- Default groups: public[28] (read only), private[29] (read/write)
- *readview* - Every object belonging to the Internet OID space (1.3.6.1).
- writeview - Nothing is defined.
- *notifyview* - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the **snmp-server user** command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- For additional information on the notification messages supported by this switch, see "Supported Notification Messages" on page 3-67. Also,

28. No view is defined.
29. Maps to the defaultview.

note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the **snmp-server enable traps** command (page 4-146).

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
```

```
Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

Table 4-40 show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read and a Write View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

- *username* - Name of user connecting to the SNMP agent. (Range: 1-32 characters)

- *groupname* - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **encrypted** - Accepts the password as encrypted input.
- **auth** - Uses SNMPv3 with authentication.
- **md5** | **sha** - Uses MD5 or SHA authentication.
- *auth-password* - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)
- **priv des56** - Uses SNMPv3 with privacy with DES56 encryption.
- *priv-password* - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the **snmp-server engine-id** command before using this configuration command.
- Before you configure a remote user, use the **snmp-server engine-id** command (page 4-147) to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve group r&d v3 auth md5
  greenpeace priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19
  v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```

show snmp user

This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 4-41 show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. You can configure any VLAN interface to be automatically assigned an IP address via DHCP. This switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or you can configure this switch to provide DHCP service directly to any client.

Table 4-42 DHCP Commands

Command Group	Function	Page
DHCP Client	Allows interfaces to dynamically acquire IP address information	4-157
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server	4-159
DHCP Server	Configures DHCP service using address pools or static bindings	4-161

DHCP Client

Table 4-43 DHCP Client Commands

Command	Function	Mode	Page
ip dhcp client-identifier	Specifies the DHCP client identifier for this switch	IC	4-157
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE	4-158

ip dhcp client-identifier

This command specifies the DCHP client identifier for the current interface. Use the **no** form to remove this identifier.

Syntax

ip dhcp client-identifier {**text** *text* | **hex** *hex*}
no ip dhcp client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of your DHCP server.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

Related Commands

ip dhcp restart client (4-158)

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.1.54, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip address (4-308)

DHCP Relay

Table 4-44 DHCP Relay Commands

Command	Function	Mode	Page
ip dhcp restart relay	Enables DHCP relay agent	IC	4-159
ip dhcp relay server	Specifies DHCP server addresses for relay	IC	4-160

ip dhcp restart relay

This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

Syntax

[**no**] **ip dhcp relay**

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip dhcp relay server (4-160)

ip dhcp relay server

This command specifies the addresses of DHCP servers to be used by the switch's DHCP relay agent. Use the **no** form to clear all addresses.

Syntax

ip dhcp relay server *address1* [*address2* [*address3* ...]]
no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-3 addresses)

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.
- To start DHCP relay service, enter the **ip dhcp restart relay** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

Related Commands

ip dhcp restart relay (4-159)

DHCP Server

Table 4-45 DHCP Server Commands

Command	Function	Mode	Page
service dhcp	Enables the DHCP server feature on this switch	GC	4-162
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients	GC	4-163
ip dhcp pool	Configures a DHCP address pool on a DHCP Server	GC	4-163
network	Configures the subnet number and mask for a DHCP address pool	DC	4-164
default-router	Specifies the default router list for a DHCP client	DC	4-165
domain-name	Specifies the domain name for a DHCP client	DC	4-166
dns-server	Specifies the Domain Name Server (DNS) servers available to a DHCP client	DC	4-167
next-server	Configures the next server in the boot process of a DHCP client	DC	4-167
bootfile	Specifies a default boot image for a DHCP client	DC	4-168

Table 4-45 DHCP Server Commands (Continued)

Command	Function	Mode	Page
netbios-name-server	Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients	DC	4-169
netbios-node-type	Configures NetBIOS node type for Microsoft DHCP clients	DC	4-170
lease	Sets the duration an IP address is assigned to a DHCP client	DC	4-171
host*	Specifies the IP address and network mask to manually bind to a DHCP client	DC	4-172
client-identifier*	Specifies a client identifier for a DHCP client	DC	4-173
hardware-address*	Specifies the hardware address of a DHCP client	DC	4-174
clear ip dhcp binding	Deletes an automatic address binding from the DHCP server database	PE	4-175
show ip dhcp binding	Displays address bindings on the DHCP server	PE, NE	4-176

* These commands are used for manually binding an address to a client.

service dhcp

This command enables the DHCP server on this switch. Use the **no** form to disable the DHCP server.

Syntax

[**no**] **service dhcp**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If the DHCP server is running, you must restart it to implement any configuration changes.

Example

```
Console(config)#service dhcp
Console(config)#
```

ip dhcp excluded-address

This command specifies IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

Syntax

[**no**] **ip dhcp excluded-address** *low-address* [*high-address*]

- *low-address* - An excluded IP address, or the first IP address in an excluded address range.
- *high-address* - The last IP address in an excluded address range.

Default Setting

All IP pool addresses may be assigned.

Command Mode

Global Configuration

Example

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

This command configures a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

Syntax

[**no**] **ip dhcp pool** *name*

name - A string or integer. (Range: 1-8 characters)

Default Setting

DHCP address pools are not configured.

Command Mode

Global Configuration

Usage Guidelines

- After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- From this mode, first configure address pools for the network interfaces (using the **network** command). You can also manually bind an address to a specific client (with the **host** command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a **host** command must fall within the range of a configured network address pool.

Example

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

Related Commands

network (4-164)
host (4-172)

network

This command configures the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

Syntax

network *network-number* [*mask*]
no network

- *network-number* - The IP address of the DHCP address pool.
- *mask* - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Command Mode

DHCP Pool Configuration

Usage Guidelines

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used (see page 3-295). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the ip **dhcp excluded-address** command.

Example

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

default-router

This command specifies default routers for a DHCP pool. Use the **no** form to remove the default routers.

Syntax

default-router *address1* [*address2*]
no default-router

- *address1* - Specifies the IP address of the primary router.
- *address2* - Specifies the IP address of an alternate router.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

Example

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

domain-name

This command specifies the domain name for a DHCP client. Use the **no** form to remove the domain name.

Syntax

domain-name *domain*
no domain-name

domain - Specifies the domain name of the client. (Range: 1-32 characters)

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

dns-server

This command specifies the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

Syntax

dns-server *address1* [*address2*]
no dns-server

- *address1* - Specifies the IP address of the primary DNS server.
- *address2* - Specifies the IP address of the alternate DNS server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

next-server

This command configures the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

Syntax

[**no**] **next-server** *address*

address - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

Related Commands

bootfile (4-168)

bootfile

This command specifies the name of the default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified with the **next-server** command. Use the **no** form to delete the boot image name.

Syntax

bootfile *filename*
no bootfile

filename - Name of the file that is used as a default boot image.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

Related Commands

next-server (4-167)

netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

Syntax

netbios-name-server *address1* [*address2*]
no netbios-name-server

- *address1* - Specifies IP address of primary NetBIOS WINS name server.
- *address2* - Specifies IP address of alternate NetBIOS WINS name server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

Related Commands

netbios-node-type (4-170)

netbios-node-type

This command configures the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

Syntax

netbios-node-type *type*
no netbios-node-type

type - Specifies the NetBIOS node type:

- **broadcast**
- **hybrid (recommended)**
- **mixed**
- **peer-to-peer**

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

Related Commands

netbios-name-server (4-169)

lease

This command configures the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

Syntax

lease {*days* [*hours*][*minutes*] | **infinite**}
no lease

- *days* - Specifies the duration of the lease in numbers of days. (Range: 0-364)
- *hours* - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)
- *minutes* - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)
- **infinite** - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

Default Setting

One day

Command Modes

DHCP Pool Configuration

Example

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

host

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

Syntax

host *address* [*mask*]
no host

- *address* - Specifies the IP address of a client.
- *mask* - Specifies the network mask of the client.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the **client-identifier** or **hardware-address** commands, then the switch will assign an address from the matching network pool.
- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see page 3-295). This command is valid for manual bindings only.

- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

Example

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

Related Commands

client-identifier (4-173)
hardware-address (4-174)

client-identifier

This command specifies the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

Syntax

client-identifier {**text** *text* | **hex** *hex*}
no client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

DHCP Pool Configuration

Command Usage

- This command identifies a DHCP client to bind to an address specified in the **host** command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.
- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

Related Commands

host (4-172)

hardware-address

This command specifies the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

Syntax

hardware-address *hardware-address type*
no hardware-address

- *hardware-address* - Specifies the MAC address of the client device.
- *type* - Indicates the following protocol used on the client device:
  - ethernet
  - ieee802
  - fddi

Default Setting

If no type is specified, the default protocol is Ethernet.

Command Mode

DHCP Pool Configuration

Command Usage

This command identifies a DHCP or BOOTP client to bind to an address specified in the **host** command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

Related Commands

host (4-172)

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database.

Syntax

clear ip dhcp binding {*address* | ***** }

- *address* - The address of the binding to clear.
- ***** - Clears all automatic bindings.

Default Setting

None

Command Mode

Privileged Exec

Usage Guidelines

- An *address* specifies the client's IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the **no host** command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

Example.

```
Console#clear ip dhcp binding *
Console#
```

Related Commands

show ip dhcp binding (4-176)

show ip dhcp binding

This command displays address bindings on the DHCP server.

Syntax

show ip dhcp binding [*address*]

address - Specifies the IP address of the DHCP client for which bindings will be displayed.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dhcp binding

     IP                MAC           Lease Time        Start
                                    (dd/hh/mm/ss)
--------------- ----------------- ----------------- --------------------
     192.1.3.21 00-00-e8-98-73-21              86400 Dec 25 08:01:57 2002
Console#
```

DNS Commands

These commands are used to configure Domain Naming System (DNS) services. You can manually configure entries in the DNS domain name to IP address mapping table, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the **ip name-server** command and domain lookup is enabled with the **ip domain-lookup** command.

Table 4-46 DNS Commands

Command	Function	Mode	Page
ip host	Creates a static host name-to-address mapping	GC	4-178
clear host	Deletes entries from the host name-to-address table	PE	4-179
ip domain-name	Defines a default domain name for incomplete host names	GC	4-179
ip domain-list	Defines a list of default domain names for incomplete host names	GC	4-180
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC	4-181
ip domain-lookup	Enables DNS-based host name-to-address translation	GC	4-182
show hosts	Displays the static host name-to-address mapping table	PE	4-183
show dns	Displays the configuration for DNS services	PE	4-184
show dns cache	Displays entries in the DNS cache	PE	4-184
clear dns cache	Clears all entries from the DNS cache	PE	4-185

ip host

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the **no** form to remove an entry.

Syntax

[**no**] **ip host** *name address1* [*address2* … *address8*]

- *name* - Name of the host. (Range: 1-64 characters)
- *address1* - Corresponding IP address.
- *address2* … *address8* - Additional corresponding IP addresses.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.

Example

This example maps two address to a host name.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
Console#
```

clear host

This command deletes entries from the DNS table.

Syntax

clear host {*name* | *}

- *name* - Name of the host. (Range: 1-64 characters)
- * - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Example

This example clears all static entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

Syntax

ip domain-name *name*
no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
Name Server List:
Console#
```

Related Commands

ip domain-list (4-180)
ip name-server (4-181)
ip domain-lookup (4-182)

ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

Syntax

[**no**] **ip domain-list** *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS server on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.

- If there is no domain list, the domain name specified with the **ip domain-name** command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
Console#
```

Related Commands

ip domain-name (4-179)

ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

[**no**] **ip name-server** *server-address1* [*server-address2* … *server-address6*]

- *server-address1* - IP address of domain-name server.
- *server-address2* … *server-address6* - IP address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name (4-179)
ip domain-lookup (4-182)

ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[**no**] **ip domain-lookup**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- At least one name server must be specified before you can enable DNS.
- If all name servers are deleted, DNS will automatically be disabled.

Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
```

Related Commands

ip domain-name (4-179)
ip name-server (4-181)

show hosts

This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```

show dns

This command displays the configuration of the DNS server.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
0        4      CNAME   10.2.44.96      893     pttch_pc.smc.com.tw
1        4      CNAME   10.2.44.3       898     ahten.smc.com.tw
2        4      CNAME   66.218.71.84    298     www.yahoo.akadns.net
3        4      CNAME   66.218.71.83    298     www.yahoo.akadns.net
4        4      CNAME   66.218.71.81    298     www.yahoo.akadns.net
5        4      CNAME   66.218.71.80    298     www.yahoo.akadns.net
6        4      CNAME   66.218.71.89    298     www.yahoo.akadns.net
7        4      CNAME   66.218.71.86    298     www.yahoo.akadns.net
8        4      ALIAS   POINTER TO:7    298     www.yahoo.com
Console#
```

Table 4-47 show dns cache - display description

Field	Description
NO	The entry number for each resource record.
FLAG	The flag is always "4" indicating a cache entry and therefore unreliable.
TYPE	This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
IP	The IP address associated with this record.
TTL	The time to live reported by the name server.
DOMAIN	The domain name associated with this record.

clear dns cache

This command clears all entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#clear dns cache
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
Console#
```

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Table 4-48 Interface Commands

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	4-187
description	Adds a description to an interface configuration	IC	4-187
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	4-188
negotiation	Enables autonegotiation of a given interface	IC	4-189
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	4-190
flowcontrol	Enables flow control on a given interface	IC	4-191
media-type	Force port type selected for combination ports	IC	4-192
shutdown	Disables an interface	IC	4-193
switchport broadcast packet-rate	Configures the broadcast storm control threshold	IC	4-194
clear counters	Clears statistics on an interface	PE	4-195
show interfaces status	Displays status for the specified interface	NE, PE	4-196
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	4-197
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-199

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

description

This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**10000full** | **1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **10000full** - Forces 10 Gbps full-duplex operation
- **1000full** - Forces 1 Gbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is:
  - Gigabit Ethernet ports – **1000full (**1 Gbps full-duplex)
  - 10 Gigabit Ethernet ports – **10000full (**10 Gbps full-duplex)

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-189)
capabilities (4-190)

negotiation

This command enables autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

[no] negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When

auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (4-190)
speed-duplex (4-188)

capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[**no**] **capabilities** {**10000full** | **1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **10000full** - Supports 10 Gbps full-duplex operation
- **1000full** - Supports 1 Gbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation

Default Setting

- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full
- 10GBASE-LR: 10000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#
```

Related Commands

negotiation (4-189)
speed-duplex (4-188)
flowcontrol (4-191)

flowcontrol[30]

This command enables flow control. Use the **no** form to disable flow control.

Syntax

[**no**] **flowcontrol**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.

30. There are interoperability problems between Flow Control and Head-of-Line (HOL) blocking for the switch ASIC; Flow Control is therefore not supported for this switch.

- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-189)
capabilities (flowcontrol, symmetric) (4-190)

media-type

This command forces the port type selected for combination ports 21-24/ 45-48. Use the **no** form to restore the default mode.

Syntax

media-type *mode*
no media-type

mode

- **copper-forced** - Always uses the built-in RJ-45 port.
- **sfp-forced** - Always uses the SFP port (even if module not installed).
- **sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

Default Setting

sfp-preferred-auto

Command Mode

Interface Configuration (Ethernet)

Example

This forces the switch to use the built-in RJ-45 port for the combination port 24.

```
Console(config)#interface ethernet 1/24
Console(config-if)#media-type copper-forced
Console(config-if)#
```

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[**no**] **shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast packet-rate

This command configures broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second.
(Range: 1000BASE - 500-262143, 10GBASE - 1041-262143)

Default Setting

Enabled for all ports
Packet-rate limit: 1000BASE - 500 pps, 10GBASE - 1041 pps

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- Broadcast control does not effect IP multicast traffic.
- The resolution for Gigabit ports is 1 packet per second (pps); i.e., any setting between 500-262143 is acceptable. However, the resolution for the 10 Gigabit port is in steps of 1041 pps.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status" on page 3-119.

Example

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A5
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Broadcast storm:        Enabled
  Broadcast storm limit:  500 packets/second
  Flow control:           Disabled
  LACP:                   Disabled
  Port security:          Disabled
  Max MAC count:          0
  Port security action:   None
  Media type:             None
Current status:
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 1000full
  Flow control type:      None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address:             00-00-AB-CD-00-00
Console#
```

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port Statistics" on page 3-145.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 4.

```
Console#show interfaces switchport ethernet 1/4
 Broadcast threshold:           Enabled, 500 packets/second
 LACP status:                   Disabled
 Ingress rate limit:            Disable, 1000M bits per second
 Egress rate limit:             Disable, 1000M bits per second
 VLAN membership mode:          Hybrid
 Ingress rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 GVRP status:                   Disabled
 Allowed VLAN:                     1(u),
 Forbidden VLAN:
Console#
```

Table 4-49 show interfaces switchport - display description

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 4-194).
LACP status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 4-206).
Ingress/Egress rate limit	Shows if rate limiting is enabled, and the current rate limit (page 4-203).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 4-250).
Ingress rule	Shows if ingress filtering is enabled or disabled (page 4-252).
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 4-251).
Native VLAN	Indicates the default Port VLAN ID (page 4-253).
Priority for untagged traffic	Indicates the default priority for untagged frames (page 4-269).
GVRP status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 4-266).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 4-254).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 4-255).

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Table 4-50 Mirror Port Commands

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	4-201
show port monitor	Shows the configuration for a mirror port	PE	4-202

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *unit*/*port* (source port)
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)
- *unit* - Stack unit. (Range: 1-8)
- *port* - Port number. (Range: 1-25/49)

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Table 4-51 Rate Limit Commands

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	4-203

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input** | **output**} [*rate*]
no rate-limit {**input** | **output**}

- **input** – Input rate
- **output** – Output rate
- *rate* – Maximum value in Mbps. (Range: 1 to 10000 Mbps)

Default Setting

- Gigabit Ethernet: 1000 Mbps
- 10 Gigabit Ethernet: 10000 Mbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 4-52 Link Aggregation Commands

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	4-187
channel-group	Adds a port to a trunk	IC (Ethernet)	4-206
Dynamic Configuration Commands			
lacp	Configures LACP for the current interface	IC (Ethernet)	4-206
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)	4-208
lacp admin-key	Configures a port's administration key	IC (Ethernet)	4-209
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)	4-210
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)	4-211

Table 4-52 Link Aggregation Commands (Continued)

Command	Function	Mode	Page
Trunk Status Display Commands			
show interfaces status port-channel	Shows trunk information	NE, PE	4-196
show lacp	Shows LACP information	PE	4-212

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/ to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.

- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-32)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[**no**] **lacp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A4
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
```

```
 Current status:
  Created by:             Lacp
  Link status:            Up
  Operation speed-duplex: 1000full
  Flow control type:      None
  Member Ports:           Eth1/10, Eth1/11, Eth1/12,
Console#
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **system-priority** *priority*
no lacp {**actor** | **partner**} **system-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **admin-key** *key*
[**no**] **lacp** {**actor** | **partner**} **admin-key**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*
[**no**] **lacp admin-key**

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **port-priority** *priority*
no lacp {**actor** | **partner**} **port-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

show lacp

This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

- *port-channel* - Local identifier for a link aggregation group. (Range: 1-32)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- **neighbors** - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Port channel: 1
---------------------------------------------------------------------
Eth 1/ 2
---------------------------------------------------------------------
  LACPDUs Sent:         10
  LACPDUs Receive:      5
  Marker Sent:          0
  Marker Receive:       0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
:
```

Table 4-53 show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.

Table 4-53 show lacp counters - display description (Continued)

Field	Description
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Port channel: 1
------------------------------------------------------------------------
Oper Key:  3
Admin Key: 0
Eth 1/ 2
------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 32768
  LACP Port Priority:   32768
  Admin Key:            3
  Oper Key:             3
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
```

Table 4-54 show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

Table 4-54 show lacp internal - display description (Continued)

Field	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Port channel 1 neighbors
------------------------------------------------------------------------
Eth 1/1
------------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    32768, 00-01-F4-78-AE-C0
  Partner Admin Port Number: 2
  Partner Oper Port Number:  2
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                distributing, collecting,
   synchronization,
                             aggregation, long timeout, LACP-activity
⋮
```

Table 4-55 show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```
Console#show lacp sysid
Port Channel     System Priority    System MAC Address
-------------------------------------------------------------------------
           1               32768     00-30-F1-8F-2C-A7
           2               32768     00-30-F1-8F-2C-A7
           3               32768     00-30-F1-8F-2C-A7
           4               32768     00-30-F1-8F-2C-A7
           5               32768     00-30-F1-8F-2C-A7
           6               32768     00-30-F1-8F-2C-A7
           7               32768     00-30-F1-D4-73-A0
           8               32768     00-30-F1-D4-73-A0
           9               32768     00-30-F1-D4-73-A0
          10               32768     00-30-F1-D4-73-A0
          11               32768     00-30-F1-D4-73-A0
          12               32768     00-30-F1-D4-73-A0
⋮
```

Table 4-56 show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 4-57 Address Table Commands

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-217
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	4-218
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-219

Table 4-57 Address Table Commands (Continued)

Command	Function	Mode	Page
mac-address-table aging-time	Sets the aging time of the address table	GC	4-220
show mac-address-table aging-time	Shows the aging time for the address table	PE	4-220

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)
  - **port-channel** *channel-id* (Range: 1-32)
- *vlan-id* - VLAN ID (Range: 1-4093)
- *action* -
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
  ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)
  - **port-channel** *channel-id* (Range: 1-32)
- *vlan-id* - VLAN ID (Range: 1-4093)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 4-58 Spanning Tree Commands

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	4-222
spanning-tree mode	Configures STP, RSTP or MSTP mode	GC	4-223
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	4-225
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	4-226
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	4-226
spanning-tree priority	Configures the spanning tree bridge priority	GC	4-227
spanning-tree path-cost method	Configures the path cost method for RSTP/MSTP	GC	4-228
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC	4-229
spanning-tree mst-configuration	Changes to MSTP configuration mode	GC	4-229
mst vlan	Adds VLANs to a spanning tree instance	MST	4-230
mst priority	Configures the priority of a spanning tree instance	MST	4-231
name	Configures the name for the multiple spanning tree	MST	4-232
revision	Configures the revision number for the multiple spanning tree	MST	4-233

Table 4-58 Spanning Tree Commands (Continued)

Command	Function	Mode	Page
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST	4-233
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC	4-234
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	4-235
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	4-236
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	4-237
spanning-tree portfast	Sets an interface to fast forwarding	IC	4-238
spanning-tree link-type	Configures the link type for RSTP/MSTP	IC	4-239
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC	4-240
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC	4-241
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	4-242
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE	4-243
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE	4-245

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **spanning-tree**

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp** | **mstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)
- **mstp** - Multiple Spanning Tree (IEEE 802.1s)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol
  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree **forward-time**

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 4-235) takes precedence over port priority (page 4-236).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree mst-configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Setting

- No VLANs are mapped to any MST instance.
- The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#
```

Related Commands

mst vlan (4-230)
mst priority (4-231)
name (4-232)
revision (4-233)
max-hops (4-233)

mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

[**no**] **mst** *instance_id* **vlan** *vlan-range*

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *vlan-range* - Range of VLANs. (Range: 1-4093)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 58 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 4-232) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each

MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance_id* **priority** *priority*
no mst *instance_id* **priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *priority* - Priority of the a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

name - Name of the spanning tree.

Default Setting

Switch's MAC address

Command Mode

MST Configuration

Command Usage

The MST region name and revision number (page 4-233) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

Related Commands

revision (4-233)

revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

Syntax

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

Default Setting

0

Command Mode

MST Configuration

Command Usage

The MST region name (page 4-232) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands

name (4-232)

max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

Default Setting

20

Command Mode

MST Configuration

Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

Syntax

[**no**] **spanning-tree spanning-disabled**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the port.
(Range: 0 for auto-configuration, or 1-200,000,000)

The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000
- 10 Gigabit Ethernet: 200-20,000

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000
- 10 Gigabit Ethernet – full duplex: 1000; trunk: 500

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 4-228) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost (4-235)

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

[**no**] **spanning-tree edge-port**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (4-238)

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

[**no**] **spanning-tree portfast**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (4-237)

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance_id* **cost** *cost*
no spanning-tree mst *instance_id* **cost**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)
- *cost* - Path cost for an interface. (Range: 1-200,000,000)

  The recommended range is -
  - Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000
  - 10 Gigabit Ethernet: 200-20,000

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000
- 10 Gigabit Ethernet – full duplex: 1000; trunk: 500

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.

- Path cost takes precedence over interface priority.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

spanning-tree mst port-priority (4-241)

spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance_id* **port-priority** *priority*
no spanning-tree mst *instance_id* **port-priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)
- *priority* - Priority for an interface. (Range: 0-240 in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree mst cost (4-240)

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance_id*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)
  - **port-channel** *channel-id* (Range: 1-32)
- *instance_id* - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the **show spanning-tree mst** *instance_id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).
- For a description of the items displayed under "Spanning-tree information," see "Configuring Global Settings" on page 3-161. For a description of the items displayed for specific interfaces, see "Displaying Interface Settings" on page 3-166.

Example

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode:                MSTP
 Spanning tree enable/disable:      enable
 Instance:                          0
 Vlans configuration:               1-4093
 Priority:                          32768
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Max hops:                          20
 Remaining hops:                    20
 Designated Root:                   32768.0.0000ABCD0000
 Current root port:                 1
 Current root cost:                 10000
 Number of topology changes:        1
 Last topology changes time (sec.): 22
 Transmission limit:                3
 Path Cost Method:                  long
---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
 Admin status:             enable
 Role:                     root
 State:                    forwarding
 External admin path cost: 10000
 Internal admin cost:      10000
 External oper path cost:  10000
 Internal oper path cost:  10000
 Priority:                 128
 Designated cost:          200000
 Designated port:          128.24
 Designated root:          32768.0.0000ABCD0000
 Designated bridge:        32768.0.0030F1552000
 Fast forwarding:          disable
 Forward transitions:      1
 Admin edge port:          enable
 Oper edge port:           disable
 Admin Link type:          auto
 Oper Link type:           point-to-point
 Spanning Tree Status:     enable
:
```

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

Command Mode

Privileged Exec

Example

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-----------------------------------------------------------------
 Configuration name: R&D
 Revision level:0

 Instance Vlans
-----------------------------------------------------------------
     1    2
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 4-59 VLAN Commands

Command Groups	Function	Page
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	4-246
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP	4-248
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	4-256

Table 4-59 VLAN Commands (Continued)

Command Groups	Function	Page
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	4-257
Configuring Protocol VLANs	Configures protocol-based VLANs based on frame type and protocol	4-259

Editing VLAN Groups

Table 4-60 Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	4-246
vlan	Configures a VLAN, including VID, name and state	VC	4-247

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (4-256)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (4-256)

Configuring VLAN Interfaces

Table 4-61 Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	4-249
switchport mode	Configures VLAN membership mode for an interface	IC	4-250
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	4-251
switchport ingress-filtering	Enables ingress filtering on an interface	IC	4-252
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	4-253
switchport allowed vlan	Configures the VLANs associated with an interface	IC	4-254
switchport gvrp	Enables GVRP for an interface	IC	4-266
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-255
switchport priority default	Sets a port priority for incoming untagged frames	IC	4-271

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (4-193)

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types (4-251)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (4-250)

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[**no**] **switchport ingress-filtering**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4093, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}
no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

- All ports are assigned to VLAN 1 by default.
- The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

Displaying VLAN Information

Table 4-62 Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	4-256
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	4-196
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-199

show vlan

This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S)
Console#
```

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This section describes commands used to configure private VlANs.

Table 4-63 Private VLAN Commands

Command	Function	Mode	Page
pvlan	Enables and configured private VLANS	GC	4-257
show pvlan	Displays the configured private VLANS	PE	4-258

pvlan

This command enables or configures a private VLAN. Use the **no** form to disable the private VLAN.

Syntax

pvlan [**up-link** *interface-list* **down-link** *interface-list*]
no pvlan

- **up-link** – Specifies an uplink interface.
- **down-link** – Specifies a downlink interface.

Default Setting

No private VLANs are defined.

Command Mode

Global Configuration

Command Usage

- A private VLAN provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port.
- Private VLANs and normal VLANs can exist simultaneously within the same switch.
- Entering the **pvlan** command without any parameters enables the private VLAN. Entering **no pvlan** disables the private VLAN.

Example

This example enables the private VLAN, and then sets port 12 as the uplink and ports 5-8 as the downlinks.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/12 down-link ethernet 1/5-8
Console(config)#
```

show pvlan

This command displays the configured private VLAN.

Command Mode

Privileged Exec

Example

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/12
Down-link port:
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
Console#
```

Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 4-64 Protocol-based VLAN Commands

Command	Function	Mode	Page
protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC	4-260
protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC	4-261
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE	4-262
show interfaces protocol-vlan protocol-group	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE	4-263

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 4-247). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the **protocol-vlan protocol-group** command (General Configuration mode).

3. Then map the protocol for each interface to the appropriate VLAN using the **protocol-vlan protocol-group** command (Interface Configuration mode).

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{**add** | **remove**} **frame-type** *frame* **protocol-type** *protocol*]
no protocol-vlan protocol-group *group-id*

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *frame*[31] - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)
- *protocol* - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: ip, arp, rarp.

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type
  ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type
  ethernet protocol-type arp
Console(config)#
```

31. SNAP frame types are not supported by this switch due to hardware limitations.

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*
no protocol-vlan protocol-group *group-id* **vlan**

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *vlan-id* - VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

Default Setting

No protocol groups are mapped for any interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as **vlan** on page 4-247), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Setting

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 ProtocolGroup ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                1      ethernet     08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

   Port     ProtocolGroup ID    Vlan ID
---------- ------------------ -----------
   Eth 1/1                  1       vlan2
Console#
```

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 4-65 GVRP and Bridge Extension Commands

Command	Function	Mode	Page
bridge-ext gvrp	Enables GVRP globally for the switch	GC	4-264
show bridge-ext	Shows the global bridge extension configuration	PE	4-265
switchport gvrp	Enables GVRP for an interface	IC	4-266
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-255
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE	4-266
garp timer	Sets the GARP timer for the selected function	IC	4-267
show garp timer	Shows the GARP timer for the selected function	NE, PE	4-268

bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **bridge-ext gvrp**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Displaying Basic VLAN Information" on page 3-186 and "Displaying Bridge Extension Capabilities" on page 3-19 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support VLAN numbers:              256
 Max support VLAN ID:                   4093
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Disabled
 GMRP:                                  Disabled
Console#
```

switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

Syntax

[**no**] **switchport gvrp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP configuration: Disabled
Console#
```

garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (4-268)

show garp timer

This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer:     20 centiseconds
 Leave timer:    60 centiseconds
 Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer (4-267)

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Table 4-66 Priority Commands

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	4-269
Priority (Layer 3 and 4)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values	4-276

Priority Commands (Layer 2)

Table 4-67 Priority Commands (Layer 2)

Command	Function	Mode	Page
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC	4-270
switchport priority default	Sets a port priority for incoming untagged frames	IC	4-271
queue bandwidth	Assigns round-robin weights to the priority queues	IC	4-272
queue cos-map	Assigns class-of-service values to the priority queues	IC	4-273
show queue mode	Shows the current queue mode	PE	4-274
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	4-275

Table 4-67 Priority Commands (Layer 2)

Command	Function	Mode	Page
show queue cos-map	Shows the class-of-service map	PE	4-275
show interfaces switchport	Displays the administrative and operational status of an interface	PE	4-199

queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 - 7 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage

of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- This switch provides eight priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1 - 15)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

This example shows how to assign WRR weights to each of the priority queues:

```
Console#configure
Console(config)#int eth 1/5
Console(config-if)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config-if)#
```

Related Commands

show queue bandwidth (4-275)

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.
  Ranges are 0 to 7, where 7 is the highest priority queue.
- *cos1 ... cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Table 4-68 Default CoS Priority Levels

Queue	0	1	2	3	4	5	6	7
Priority	2	0	1	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

Example

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

Related Commands

show queue cos-map (4-275)

show queue mode

This command shows the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#sh queue mode

Wrr status: Enabled
Console#
```

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0         1
    1         2
    2         4
    3         6
    4         8
    5         10
    6         12
    7         14
:
```

show queue cos-map

This command shows the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

Priority Commands (Layer 3 and 4)

Table 4-69 Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip port	Enables TCP/UDP class of service mapping	GC	4-276
map ip port	Maps TCP/UDP socket to a class of service	IC	4-277
map ip precedence	Enables IP precedence class of service mapping	GC	4-278
map ip precedence	Maps IP precedence value to a class of service	IC	4-278
map ip dscp	Enables IP DSCP class of service mapping	GC	4-279
map ip dscp	Maps IP DSCP value to a class of service	IC	4-280
show map ip port	Shows the IP port map	PE	4-281
show map ip precedence	Shows the IP precedence map	PE	4-282
show map ip dscp	Shows the IP DSCP map	PE	4-283

map ip port (Global Configuration)

This command enables IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

[**no**] **map ip port**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

This command sets IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Global Configuration)

This command enables IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

[**no**] **map ip precedence**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping.

Table 4-70 Mapping IP Precedence to CoS Values

IP Precedence Value	0	1	2	3	4	5	6	7
CoS Value	0	1	2	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

[no] map ip dscp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-63)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 4-71 Mapping IP DSCP to CoS Values

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip port

This command shows the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Related Commands

map ip port (Global Configuration) (4-276)
map ip port (Interface Configuration) (4-277)

show map ip precedence

This command shows the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (4-278)
map ip precedence (Interface Configuration) (4-278)

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
⋮
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (4-279)
map ip dscp (Interface Configuration) (4-280)

Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 4-72 Quality of Service Commands

Command	Function	Mode	Page
class-map	Creates a class map for a type of traffic	GC	4-286
match	Defines the criteria used to classify traffic	CM	4-287
policy-map	Creates a policy map for multiple interfaces	GC	4-289
class	Defines a traffic classification for the policy to act on	PM	4-290
set	Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in a packet	PM-C	4-291
police	Defines an enforcer for classified traffic	PM-C	4-292

Table 4-72 Quality of Service Commands (Continued)

Command	Function	Mode	Page
service-policy	Applies a policy map defined by the **policy-map** command to the input of a particular interface	IC	4-293
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE	4-294
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE	4-294
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE	4-295

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the **class-map** command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the **match** command to select a specify type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Set an ACL mask to enable filtering for the criteria specified in the **match** command.
4. Use the **policy-map** command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
5. Use the **class** command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain multiple class statements.
6. Use the **set** command to modify the QoS value for matching traffic class, and use the **policer** command to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
7. Use the **service-policy** command to assign a policy map to a specific interface.

Notes: 1. You can only configure one rule per Class Map. However, you can include multiple classes in a Policy Map.
2. You must create a Class Map before creating a Policy Map.

class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map and return to Global configuration mode.

Syntax

[**no**] **class-map** *class-map-name* [**match-any**]

- **match-any** - Match any condition within a class map.
- *class-map-name* - Name of the class map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use the **match** command (page 4-287) to specify the criteria for ingress traffic that will be classified under this class map.
- Only one **match** command is permitted per class map, so the **match-any** field refers to the criteria specified by the lone **match** command for a class map.
- The class map uses the Access Control List filtering engine, so you must also set an ACL mask to enable filtering for the criteria specified in the **match** command. See "mask (IP ACL)" on page 4-123 or "mask (MAC ACL)" on page 4-133 for information on configuring an appropriate ACL mask.
- The class map is used with a policy map (page 4-289) to create a service policy (page 4-293) for a specific interface that defines packet classification, service tagging, and bandwidth policing.

Example

This example creates a class map call "rd_class," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any dscp
Console(config-ip-mask-acl)#
```

Related Commands

show class map (4-294)

match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

Syntax

[**no**] **match** {**access-list** *acl-name* | **ip dscp** *dscp* | **ip precedence** *ip-precedence* | **vlan** *vlan*}

- *acl-name* - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- *dscp* - A DSCP value. (Range: 0-63)
- *ip-precedence* - An IP Precedence value. (Range: 0-7)
- *vlan* - A VLAN. (Range:1-4094)

Default Setting

None

Command Mode

Class Map Configuration

Command Usage

- First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use the **match** command to specify the fields within ingress packets that must match to qualify for this class map.

- Only one **match** command can be entered per class map.
- The class map uses the Access Control List filtering engine, so you must also set an ACL mask to enable filtering for the criteria specified in the **match** command. See "mask (IP ACL)" on page 4-123 and "mask (MAC ACL)" on page 4-133 for information on configuring an appropriate ACL mask.

Example

This example creates a class map called "rd_class#1," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any dscp
Console(config-ip-mask-acl)#
```

This example creates a class map call "rd_class#2," and sets it to match packets marked for IP Precedence service value 5:

```
Console(config)#class-map rd_class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any precedence
Console(config-ip-mask-acl)#
```

This example creates a class map call "rd_class#3," and sets it to match packets marked for VLAN 1:

```
Console(config)#class-map rd_class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#exit
Console(config)#access-list mac mask-precedence in
Console(config-ip-mask-acl)#mask any any vid 1
Console(config-ip-mask-acl)#
```

policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map and return to Global configuration mode.

Syntax

[**no**] **policy-map** *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command (page 4-293).
- You must create a Class Map (page 4-289) before assigning it to a Policy Map.

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map and return to Policy Map configuration mode.

Syntax

[**no**] **class** *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Policy Map Configuration

Command Usage

- Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** and **police** commands to specify the match criteria, where the:
  - **set** command classifies the service that an IP packet will receive.
  - **police** command defines the maximum throughput, burst rate, and the action that results from a policy violation.
- Currently you may only configure one rule per Class Map, but you can assign one or more classes to a policy map.

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

This command services IP traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified by the **match** command on page 4-287). Use the **no** form to remove the traffic classification.

Syntax

[**no**] **set** {**cos** *new-cos* | **ip dscp** *new-dscp* | **ip precedence** *new-precedence*}

- *new-cos* - New Class of Service (CoS) value. (Range: 0-7)
- *new-dscp* - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)
- *new-precedence* - New IP Precedence value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

This command defines an policer for classified traffic. Use the **no** form to remove a policer.

Syntax

[**no**] **police** *rate-kbps burst-byte* [**exceed-action** {**drop** | **set**}]

- *rate-kbps* - Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
- *burst-byte* - Burst in bytes. (Range: 64-1522 bytes)
- **drop** - Drop packet when specified rate or burst are exceeded.
- **set** - Set DSCP service to the specified value. (Range: 0-63)

Default Setting

Drop out-of-profile packets.

Command Mode

Policy Map Class Configuration

Command Usage

- You can configure up to 63 policers (i.e., class maps) for Fast Ethernet and Gigabit Ethernet ingress ports, and up to 225 policers for 10G Ethernet ingress ports.
- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *burst-byte* field, and the average rate tokens are removed from the bucket is by specified by the *rate-bps* option.

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

This command applies a policy map defined by the **policy-map** command to the ingress queue of a particular interface. Use the **no** form to remove the policy map from this interface.

Syntax

[**no**] **service-policy input** *policy-map-name*

- **input** - Apply to the input traffic.
- *policy-map-name* - Name of the policy map for this interface. (Range: 1-32 characters)

Default Setting

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can only assign one policy map to an interface.
- You must first define a class map, set an ACL mask to match the criteria defined in the class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.

Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all class maps.

Command Mode

Privileged Exec

Example

```
Console#show class-map
Class Map match-any rd_class#1
 Match ip dscp 3

Class Map match-any rd_class#2
 Match ip precedence 5

Class Map match-any rd_class#3
 Match vlan 1

Console#
```

show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

- *policy-map-name* - Name of the policy map. (Range: 1-32 characters)
- *class-map-name* - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all policy maps and all classes.

Command Mode

Privileged Exec

Example

```
Console#show policy-map
Policy Map rd_policy
 class rd_class
  set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
 class rd_class
  set ip dscp 3
Console#
```

show policy-map interface

This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface *interface* **input**

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-25/49)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 4-73 Multicast Filtering Commands

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	4-296
IGMP Query (Layer 2)	Configures IGMP query parameters for multicast filtering at Layer 2	4-300
Static Multicast Routing	Configures static multicast router ports	4-305

IGMP Snooping Commands

Table 4-74 IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	4-297
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	4-297
ip igmp snooping version	Configures the IGMP version for snooping	GC	4-298
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	4-299
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	4-299

ip igmp snooping

This command enables IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping**

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)
  - **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

This command shows the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Configuring IGMP Snooping and Query Parameters" on page 3-228 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status:           Enabled
 Querier status:           Disabled
 Query count:              2
 Query interval:           125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version:   Version 2
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4093)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3       Eth1/11    IGMP
Console#
```

IGMP Query Commands (Layer 2)

Table 4-75 IGMP Query Commands (Layer 2)

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	4-301
ip igmp snooping query-count	Configures the query count	GC	4-301
ip igmp snooping query-interval	Configures the query interval	GC	4-302
ip igmp snooping query-max-response-time	Configures the report delay	GC	4-303
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	4-304

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping querier**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max- response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (4-303)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-25)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (4-298)
ip igmp snooping query-max-response-time (4-303)

ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (4-298)

Static Multicast Routing Commands

Table 4-76 Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	4-305
show ip igmp snooping mrouter	Shows multicast router ports	PE	4-306

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)
  - **port-channel** *channel-id* (Range: 1-32)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
Console#
```

IP Interface Commands

There are no IP addresses assigned to this router by default. You must manually configure a new address to manage the router over your network or to connect the router to existing IP subnets. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP. These commands are used to connect subnetworks to the enterprise network.

Table 4-77 IP Interface Commands

Command Group	Function	Page
Basic IP Configuration	Configures the IP address for interfaces and the gateway router	4-307
Address Resolution Protocol (ARP)	Configures static, dynamic and proxy ARP service	4-313

Basic IP Configuration

Table 4-78 Basic IP Configuration Commands

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	4-308
ip default-gateway	Defines the default gateway through which this router can reach other subnetworks	GC	4-310
show ip interface	Displays the IP settings for this device	PE	4-311
show ip redirects	Displays the default gateway configured for this device	PE	4-311
ping	Sends ICMP echo request packets to another node on the network	NE, PE	4-312

ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**} [*secondary*]
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.
- *secondary* - Specifies a secondary IP address.

Default Setting

DHCP

Command Mode

Interface Configuration (VLAN)

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.
- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- You must assign an IP address to this device to gain management access over the network or to connect the router to existing IP subnets. You can manually configure a specific IP address, or direct the device to obtain

an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.

- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can be accessed via this interface.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart client** command, or by rebooting the router.

Notes: **1.** Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router via any of these IP addresses.

2. Before you can change the primary IP address on an interface, you must first clear the current address with the no form of this command.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart client (4-158)

ip default-gateway

This command specifies the default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

- The gateway specified in this command is only valid if routing is disabled with the **no ip routing** command. If IP routing is disabled, you must define a gateway if the target device is located in a different subnet.
- If routing is enabled, you must define the gateway with the **ip route** command.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects (4-311)
ip routing (4-318)
ip route (4-319)

show ip interface

This command displays the settings of an IP interface.

Command Mode

Privileged Exec

Example

```
Console#show ip interface

Vlan 1 is up, addressing mode is User
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

show ip redirects (4-311)

show ip redirects

This command shows the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (4-310)

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5
   seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (4-187)

Address Resolution Protocol (ARP)

Table 4-79 Address Resolution Protocol Commands

Command	Function	Mode	Page
arp	Adds a static entry in the ARP cache	GC	4-314
arp-timeout	Sets the time a dynamic entry remains in the ARP cache	GC	4-315
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE	4-315
show arp	Displays entries in the ARP cache	NE, PE	4-316
ip proxy-arp	Enables proxy ARP service	VC	4-316

arp

This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*
no arp *ip-address*

- *ip-address* - IP address to map to a specified hardware address.
- *hardware-address* - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting

No default entries

Command Mode

Global Configuration

Command Usage

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is 128.
- You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

clear arp-cache
show arp

arp-timeout

This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default.

Syntax

arp-timeout *seconds*
no arp-timeout

seconds - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 is one day)

Default Setting

1200 seconds (20 minutes)

Command Mode

Global Configuration

Command Usage

Use the **show arp** command to display the current cache timeout value.

Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp-timeout 900
Console(config)#
```

clear arp-cache

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

Privileged Exec

Example

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

Use this command to display entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the corresponding IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this router.

Example

This example displays all entries in the ARP cache.

```
Console#show arp
Arp cache timeout: 1200 (seconds)

    IP Address       MAC Address      Type   Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other           1
     10.1.0.254 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1
  123.20.10.123 02-10-20-30-40-50    static           2
   345.30.20.23 09-50-40-30-20-10   dynamic           3

Total entry : 5
Console#
```

ip proxy-arp

This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

Syntax

[no] ip proxy-arp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

Example

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

IP Routing Commands

After you configure network interfaces for this router, you must set the paths used to send traffic between different interfaces. If you enable routing on this device, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, you can either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Table 4-80 IP Routing Commands

Command Group	Function	Page
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table, and statistics for protocols used to exchange routing information	4-318
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP	4-324
Open Shortest Path First (OSPF)	Configures global and interface specific parameters for OSPF	4-338

Global Routing Configuration

Table 4-81 Global Routing Configuration Commands

Command	Function	Mode	Page
ip routing	Enables static and dynamic IP routing	GC	4-318
ip route	Configures static routes	GC	4-319
clear ip route	Deletes specified entries from the routing table	PE	4-320
show ip route	Displays specified entries in the routing table	PE	4-320
show ip host-route	Displays displays the interface associated with known routes	PE	4-322
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE	4-323

ip routing

This command enables IP routing. Use the **no** form to disable IP routing.

Syntax

[no] ip routing

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- The command affects both static and dynamic unicast routing.
- If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

Example

```
Console(config)#ip routing
Console(config)#
```

ip route

This command configures static routes. Use the **no** form to remove static routes.

Syntax

ip route {*destination-ip netmask* | **default**} {*gateway*} [**metric** *metric*]
no ip route {*destination-ip netmask* | **default** | *****}

- *destination-ip* – IP address of the destination network, subnetwork, or host.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **default** – Sets this entry as the default route.
- *gateway* – IP address of the gateway used for this route.
- *metric* – Selected RIP cost for this interface. (Range: 1-5, default: 1)
- ***** – Removes all static routing table entries.

Default Setting

No static routes are configured.

Command Mode

Global Configuration

Command Usage

- You can configure up to 2000 static routes.
- Static routes take precedence over dynamically learned routes.
- Static routes are included in RIP updates periodically sent by the router.

Example

This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

clear ip route

This command removes dynamically learned entries from the IP routing table.

Syntax

clear ip route {*network* [*netmask*] | ***}

- *network* – Network or subnet address.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- * – Removes all dynamic routing table entries.

Command Mode

Privileged Exec

Command Usage

- This command only clears dynamically learned routes.
- Use the **no ip address** command to remove a local interface.
- Use the **no ip route** command to remove a static route.

Example

```
Console#clear ip route 10.1.5.0
Console#
```

show ip route

This command displays information in the IP routing table.

Syntax

show ip route [**config** | *address* [*netmask*]]

- **config** – Displays all static routing entries.
- *address* – IP address of the destination network, subnetwork or host for which routing information is to be displayed.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

Command Mode

Privileged Exec

Command Usage

If the *address* is specified without the *netmask* parameter, the router displays all routes for the corresponding natural class address (page 4-327).

Example

```
Console#show ip route

  Ip Address        Netmask        Next Hop      Protocol  Metric Interface
-------------- -------------- --------------- ---------- ------ ---------
        0.0.0.0        0.0.0.0     10.2.48.102     static      0         1
      10.2.48.2  255.255.252.0      10.2.48.16      local      0         1
       10.2.5.6  255.255.255.0       10.2.8.12        RIP      1         2
       10.3.9.1  255.255.255.0      10.2.9.254 OSPF-intra      2         3


Total entry: 4
Console#
```

Table 4-82 show ip route - display description

Field	Description
Ip Address	IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
Netmask	Network mask for the associated IP subnet.
Next Hop	IP address of the next hop (or gateway) used for this route.
Protocol	The protocol which generated this route information. (Values: static, local, RIP, OSPF)
Metric	Cost for this interface.
Interface	VLAN interface through which this address can be reached.

show ip host-route

This command displays the interface associated with known routes.

Command Mode

Privileged Exec

Example

```
Console#show ip host-route
Total count: 0
  IP address               Mac address            VLAN     Port
  -------------------      -------------------    ------   ------
  192.168.  1.250          00-00-30-01-01-01         3     1/ 1
   10.  2. 48.  2          00-00-30-01-01-02         1     1/ 1
   10.  2.  5.  6          00-00-30-01-01-03         1     1/ 2
   10.  3.  9.  1          00-00-30-01-01-04         2     1/ 3

Console#
```

Table 4-83 show ip host-route - display description

Field	Description
Ip address	IP address of the destination network, subnetwork, or host.
Mac address	The physical layer address associated with the IP address.
VLAN	The VLAN that connects to this IP address.
Port	The port that connects to this IP address.

show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

Privileged Exec

Command Usage

For a description of the information shown by this command, see "Displaying Statistics for IP Protocols" on page 3-282.

Example

```
Console#show ip traffic
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#
```

Routing Information Protocol (RIP)

Table 4-84 Routing Information Protocol Commands

Command	Function	Mode	Page
router rip	Enables the RIP routing protocol	GC	4-325
timers basic	Sets basic timers, including update, timeout, garbage collection	RC	4-325
network	Specifies the network interfaces that are to use RIP routing	RC	4-327
neighbor	Defines a neighboring router with which to exchange information	RC	4-328
version	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC	4-328
ip rip receive version	Sets the RIP receive version to use on a network interface	IC	4-330
ip rip send version	Sets the RIP send version to use on a network interface	IC	4-331
ip split-horizon	Enables split-horizon or poison-reverse loop prevention	IC	4-332
ip rip authentication key	Enables authentication for RIP2 packets and specifies keys	IC	4-333
ip rip authentication mode	Specifies the type of authentication used for RIP2 packets	IC	4-334
show rip globals	Displays global configuration settings and statistics for RIP	PE	4-335
show ip rip	Displays RIP configuration information for each network interface	PE	4-336

router rip

This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

[**no**] **router rip**

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router rip
Console(config-router)#
```

Related Commands

network (4-327)

timers basic

This command configures the RIP update timer, timeout timer, and garbage-collection timer. Use the **no** form to restore the defaults.

Syntax

timers basic *update-seconds*
no timers basic

update-seconds – Sets the update timer to the specified value, sets the timeout time value to 6 times the update time, and sets the garbage-collection timer to 4 times the update time.
(Range for update timer: 15-60 seconds)

Command Mode

Router Configuration

Default Setting

- Update: 30 seconds
- Timeout: 180 seconds
- Garbage collection: 120 seconds

Command Usage

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging it.
- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- These timers must be set to the same values for all routers in the network.

Example

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

network

This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

Syntax

[**no**] **network** *subnet-address*

subnet-address – IP address of a network directly connected to this router.

Command Mode

Router Configuration

Default Setting

No networks are specified.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:
  - 0 - 127 is class A, and only the first field in the network address is used.
  - 128 - 191 is class B, and the first two fields in the network address are used.
  - 192 - 223 is class C, and the first three fields in the network address are used.

Example

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

Related Commands

router rip (4-325)

neighbor

This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

Syntax

[**no**] **neighbor** *ip-address*

ip-address - IP address to map to a specified hardware address.

Command Mode

Router Configuration

Default Setting

No neighbors are defined.

Command Usage

This command can be used to configure a static neighbor with which this router will exchange information, rather than relying on broadcast messages generated by the RIP protocol.

Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

version

This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

Syntax

version {**1** | **2**}
no version

- **1** - RIP Version 1
- **2** - RIP Version 2

Command Mode

Router Configuration

Default Setting

RIP Version 1

Command Usage

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the following values:
  - RIP Version 1 configures the unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures the unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the default send or receive version.

Example

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

Related Commands

ip rip receive version (4-330)
ip rip send version (4-331)

ip rip receive version

This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

Syntax

ip rip receive version {**none** | **1** | **2** | **1 2**}
no ip rip receive version

- **none** - Does not accept incoming RIP packets.
- **1** - Accepts only RIPv1 packets.
- **2** - Accepts only RIPv2 packets.
- **1 2** - Accepts RIPv1 or RIPv2 packets

Command Mode

Interface Configuration (VLAN)

Default Setting

The default depends on the setting specified with the **version** command:

- Global RIPv1 - RIPv1 or RIPv2 packets
- Global RIPv2 - RIPv2 packets

Command Usage

- Use this command to override the global setting specified by the RIP **version** command.
- You can specify the receive version based on these options:
  - Use "none" if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
  - Use "1" or "2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "1 2" if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

Example

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

Related Commands

version (4-328)

ip rip send version

This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

Syntax

ip rip send version {**none** | **1** | **2** | **v2-broadcast**}
no ip rip send version

- **none** - Does not transmit RIP updates.
- **1** - Sends only RIPv1 packets.
- **2** - Sends only RIPv2 packets.
- **v2-broadcast** - Route information is broadcast to other routers with RIPv2.

Command Mode

Interface Configuration (VLAN)

Default Setting

The default depends on the setting specified with the **version** command:

- Global RIPv1 - Route information is broadcast to other routers with RIPv2
- Global RIPv2 - RIPv2 packets

Command Usage

- Use this command to override the global setting specified by the RIP **version** command.

- You can specify the receive version based on these options:
  - Use "none" to passively monitor route information advertised by other routers attached to the network.
  - Use "1" or "2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "v2-broadcast" to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)

Example

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

Related Commands

version (4-328)

ip split-horizon

This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable split-horizon.

Syntax

ip split-horizon [**poison-reverse**]
no ip split-horizon

poison-reverse - Enables poison-reverse on the current interface.

Command Mode

Interface Configuration (VLAN)

Default Setting

split-horizon

Command Usage

- Split horizon never propagates routes back to an interface from which they have been acquired.
- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)

Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

ip rip authentication key

This command enables authentication for RIPv2 packets and to specify the key that must be used on an interface. Use the **no** form to prevent authentication.

Syntax

ip rip authentication key *key-string*
no ip rip authentication

key-string - A password used for authentication. (Range: 1-16 characters, case sensitive)

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password.

Example

This example sets an authentication password of "small" to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication key small
Console(config-if)#
```

Related Commands

ip rip authentication mode (4-334)

ip rip authentication mode

This command specifies the type of authentication that can be used on an interface. Note that the current firmware version only supports a simple password. Use the **no** form to restore the default value.

Syntax

ip rip authentication mode {**text**}
no ip rip authentication mode

text - Indicates that a simple password will be used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- The password to be used for authentication is specified in the **ip rip authentication key** command (page 4-333).
- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

Related Commands

ip rip authentication key (4-333)

show rip globals

This command displays global configuration settings for RIP.

Command Mode

Privileged Exec

Example

```
Console#show rip globals

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 0
Number of Queries: 1
Console#
```

Table 4-85 show rip globals - display description

Field	Description
RIP Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.

show ip rip

This command displays information about interfaces configured for RIP.

Syntax

show ip rip {**configuration** | **status** | **peer**}

- **configuration** - Shows RIP configuration settings for each interface.
- **status** - Shows the status of routing messages on each interface.
- **peer** - Shows information on neighboring routers, along with information about the last time a route update was received, the RIP version used by the neighbor, and the status of routing messages received from this neighbor.

Command Mode

Privileged Exec

Example

```
Console#show ip rip configuration

     Interface      SendMode      ReceiveMode     Poison       Authentication
-------------- --------------- ------------- -------------- ------------------
     10.1.0.253  rip1Compatible     RIPv1Orv2   SplitHorizon   noAuthentication
     10.1.1.253  rip1Compatible     RIPv1Orv2   SplitHorizon   noAuthentication
Console#show ip rip status

     Interface   RcvBadPackets   RcvBadRoutes     SendUpdates
-------------- --------------- -------------- ---------------
     10.1.0.253               0              0              13
     10.1.1.253               0              0              13
Console#show ip rip peer

          Peer   UpdateTime   Version   RcvBadPackets   RcvBadRoutes
-------------- ------------ --------- --------------- --------------
     10.1.0.254         1625         2               0              0
     10.1.1.254         1625         2               0              0
Console#
```

Table 4-86 show ip rip - display description

Field	Description
show ip rip configuration	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, or RIPv2-broadcast)
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1 or RIPv2)
Poison	Shows if split-horizon, poison-reverse, or no protocol message loopback prevention method is in use.
Authentication	Shows if authentication is set to simple password or none.
show ip rip status	
Interface	IP address of the interface.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
show ip rip peer	
Peer	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Open Shortest Path First (OSPF)

Table 4-87 Open Shortest Path First Commands

Command	Function	Mode	Page
General Configuration			
router ospf	Enables or disables OSPF	GC	4-340
router-id	Sets the router ID for this device	RC	4-340
compatible rfc1583	Calculates summary route costs using RFC 1583 (OSPFv1)	RC	4-341
default-information originate	Generates a default external route into an autonomous system	RC	4-342
timers spf	Configures the hold time between consecutive SPF calculations	RC	4-343
Route Metrics and Summaries			
area range	Summarizes routes advertised by an ABR	RC	4-344
area default-cost	Sets the cost for a default summary route sent into a stub or NSSA	RC	4-345
summary-address	Summarizes routes advertised by an ASBR	RC	4-346
redistribute	Redistribute routes from one routing domain to another	RC	4-347
Area Configuration			
network area	Assigns specified interface to an area	RC	4-348
area stub	Defines a stubby area that cannot send or receive LSAs	RC	4-350
area nssa	Defines a not-so-stubby that can import external routes	RC	4-351
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC	4-353
Interface Configuration			
ip ospf authentication	Specifies the authentication type for an interface	IC	4-356
ip ospf authentication-key	Assigns a simple password to be used by neighboring routers	IC	4-357
ip ospf message-digest-key	Enables MD5 authentication and sets the key for an interface	IC	4-358

Table 4-87 Open Shortest Path First Commands (Continued)

Command	Function	Mode	Page
ip ospf cost	Specifies the cost of sending a packet on an interface	IC	4-359
ip ospf dead-interval	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC	4-360
ip ospf hello-interval	Specifies the interval between sending hello packets	IC	4-361
ip ospf priority	Sets the router priority used to determine the designated router	IC	4-361
ip ospf retransmit-interval	Specifies the time between resending a link-state advertisement	IC	4-362
ip ospf transmit-delay	Estimates time to send a link-state update packet over an interface	IC	4-363
Display Information			
show ip ospf	Displays general information about the routing processes	PE	4-364
show ip ospf border-routers	Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR)	PE	4-365
show ip ospf database	Shows information about different LSAs in the database	PE	4-366
show ip ospf interface	Displays interface information	PE	4-375
show ip ospf neighbor	Displays neighbor information	PE	4-376
show ip ospf summary-address	Displays all summary address redistribution information	PE	4-377
show ip ospf virtual-links	Displays parameters and the adjacency state of virtual links	PE	4-378

router ospf

This command enables Open Shortest Path First (OSPF) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

[**no**] **router ospf**

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- OSPF is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router ospf
Console(config-router)#
```

Related Commands

network area (4-348)

router-id

This command assigns a unique router ID for this device within the autonomous system. Use the **no** form to use the default router identification method (i.e., the lowest interface address).

Syntax

router-id *ip-address*
no router-id

ip-address - Router ID formatted as an IP address.

Command Mode

Router Configuration

Default Setting

Lowest interface address

Command Usage

- The router ID must be unique for every router in the autonomous system. Using the default setting based on the lowest interface address ensures that each router ID is unique. Also, note that you cannot set the router ID to 0.0.0.0 or 255.255.255.255.
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.
- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

Example

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

Related Commands

router ospf (4-340)

compatible rfc1583

This command calculates summary route costs using RFC 1583 (OSPFv1). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

Syntax

[**no**] **compatible rfc1583**

Command Mode

Router Configuration

Default Setting

RFC 1583 compatible

Command Usage

All routers in an OSPF routing domain should use the same RFC for calculating summary routes.

Example

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate

This command generates a default external route into an autonomous system. Use the **no** form to disable this feature.

Syntax

default-information originate [**always**] [**metric** *interface-metric*] [**metric-type** *metric-type*]
no default-information originate

- **always** - Always advertise a default route to the local AS regardless of whether the router has a default route. (See "ip route" on page 4-319.)
- *interface-metric* - Metric assigned to the default route. (Range: 1-65535; Default: 10)
- *metric-type* - External link type used to advertise the default route. (Options: Type 1, Type 2; Default: Type 2)

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.
- When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.
  - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. (To define a default route, use the **ip route** command.)

- If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the **redistribute** command is used to import external routes via RIP or static routing, and such a route is known.

• Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

Example

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20
   metric-type 2
Console(config-router)#
```

Related Commands

ip route (4-319)
redistribute (4-347)

timers spf

This command configures the hold time between making two consecutive shortest path first (SPF) calculations. Use the **no** form to restore the default value.

Syntax

timers spf *spf-holdtime*
no timers spf

spf-holdtime - Minimum time between two consecutive SPF calculations. (Range: 0-65535 seconds)

Command Mode

Router Configuration

Default Setting

10 seconds

Command Usage

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

Example

```
Console(config-router)#timers spf 20
Console(config-router)#
```

area range

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

Syntax

[**no**] **area** *area-id* **range** *ip-address netmask* [**advertise** | **not-advertise**]

- *area-id* - Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- *ip-address* - Base address for the routes to summarize.
- *netmask* - Network mask for the summary route.
- **advertise** - Advertises the specified address range.
- **not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- This command can be used to advertise routes between areas.
- If routes are set to be advertised, the router will issue a Type 3 summary LSA for each address range specified with this command.
- This router supports up 64 summary routes for area ranges.

Example

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0
   advertise
Console(config-router)#
```

area default-cost

This command specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

Syntax

area *area-id* **default-cost** *cost*
no area *area-id* **default-cost**

- *area-id* - Identifier for a stub or NSSA, in the form of an IP address.
- *cost* - Cost for the default summary route sent to a stub or NSSA. (Range: 0-65535)

Command Mode

Router Configuration

Default Setting

1

Command Usage

- If you enter this command for a normal area, it will changed to a stub.
- If the default cost is set to "0," the router will not advertise a default route into the attached stub or NSSA.

Example

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

Related Commands

area stub (4-350)

summary-address

This command aggregates routes learned from other protocols. Use the **no** form to remove a summary address.

Syntax

[**no**] **summary-address** *summary-address netmask*

- *summary-address* - Summary address covering a range of addresses.
- *netmask* - Network mask for the summary route.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems.
- This router supports up 16 Type-5 summary routes.

Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

Related Commands

area range (4-344)

redistribute

This command imports external routing information from other routing domains (i.e., protocols) into the autonomous system. Use the **no** form to disable this feature.

Syntax

[**no**] **redistribute** [**rip** | **static**] [**metric** *metric-value*] [**metric-type** *type-value*]

- **rip** - External routes will be imported from the Routing Information Protocol into this Autonomous System.
- **static** - Static routes will be imported into this Autonomous System.
- *metric-value* - Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)
- *type-value*
  - **1** - Type 1 external route
  - **2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

Command Mode

Router Configuration

Default Setting

- redistribution - none
- protocol - RIP and static
- metric-value - 0
- type-metric - 2

Command Usage

- This router supports redistribution for both RIP and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the **default-information originate** command to generate a "default" external route into the AS, the metric value specified in this command supersedes the metric specified in the **default-information originate** command.

- Metric type specifies the way to advertise routes to destinations outside the AS via External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.

Example

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

Related Commands

default-information originate (4-342)

network area

This command defines an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

Syntax

[**no**] **network** *ip-address netmask* **area** *area-id*

- *ip-address* - Address of the interfaces to add to the area.
- *netmask* - Network mask of the address range to add to the area.
- *area-id* - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- Be sure to include the primary address for an interface in the network area, otherwise, OSPF will not operate for any secondary addresses covered by the command.
- An interface can only be assigned to a single area. If an address range is overlapped in subsequent network area commands, the router will implement the address range for the area specified in first command, and ignore the overlapping ranges in subsequent commands. However, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.
- This router supports up to 64 OSPF router interfaces, and up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

Syntax

[**no**] **area** *area-id* **stub** [**summary**]

- *area-id* - Identifies the stub area.
  (The area ID must be in the form of an IP address.)
- **summary** - Makes an Area Border Router (ABR) send a summary link advertisement into the stub area. (Default: no summary)

Command Mode

Router Configuration

Default Setting

No stub is configured.

Command Usage

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- Use the **area default-cost** command to specify the cost of a default summary route sent into a stub by an ABR.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

Related Commands

area default-cost (4-345)

area nssa

This command defines a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

Syntax

[**no**] **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]

- *area-id* - Identifies the NSSA. (The area ID must be in the form of an IP address.)
- **no-redistribution** - Use this keyword when the router is an NSSA Area Border Router (ABR) and you want the **redistribute** command to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.
- **default-information-originate** - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

Command Mode

Router Configuration

Default Setting

No NSSA is configured.

Command Usage

- All routers in a NSSA must be configured with the same area ID.
- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the

default- information-originate keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.

- External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa
   default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

Syntax

[**no**] **area** *area-id* **virtual-link** *router-id*
[**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [[**authentication-key** *key*] | [**message-digest-key** *key-id* **md5** *key*]]
no area *area-id*

- *area-id* - Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- *router-id* - Router ID of the virtual link neighbor. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area at the other end of the virtual link.
- **authentication** - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.
- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.
- **hello-interval** *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)
- **retransmit-interval** *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce

unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)

- **transmit-delay** *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-3600 seconds; Default: 1 seconds)
- **dead-interval** *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)
- **authentication-key** *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.
- **message-digest-key** *key-id* **md5** *key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 1-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

Command Mode

Router Configuration

Default Setting

- *area-id*: None
- *router-id*: None
- **hello-interval**: 10 seconds
- **retransmit-interval**: 5 seconds
- **transmit-delay**: 1 second
- **dead-interval**: 40 seconds

- **authentication-key**: None
- **message-digest-key**: None

Command Usage

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area. You can specify up to 32 virtual links on this router.
- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.
- This router supports up 64 virtual links.

Example

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
   message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

Related Commands

show ip ospf virtual-links (4-378)

ip ospf authentication

This command specifies the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

Syntax

ip ospf authentication [**message-digest** | **null**]
no ip ospf authentication

- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- The plain-text authentication-key, or the MD5 key-id and key, must be used consistently throughout the autonomous system.

Example

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

Related Commands

ip ospf authentication-key (4-357)
ip ospf message-digest-key (4-358)

ip ospf authentication-key

This command assigns a simple password to be used by neighboring routers. Use the **no** form to remove the password.

Syntax

ip ospf authentication-key *key*
no ip ospf authentication-key

key - Sets a plain text password. (Range: 1-8 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

No password

Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- A different password can be assigned to each network interface basis, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

Example

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

Related Commands

ip ospf authentication (4-356)

ip ospf message-digest-key

This command enables message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

Syntax

ip ospf message-digest-key *key-id* **md5** *key*
no ip ospf message-digest-key *key-id*

- *key-id* - Index number of an MD5 key. (Range: 1-255)
- *key* - Alphanumeric password used to generate a 128 bit message digest or "fingerprint." (Range: 1-16 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

MD5 authentication is disabled.

Command Usage

- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Example

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

Related Commands

ip ospf authentication (4-356)

ip ospf cost

This command explicitly sets the cost of sending a packet on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf cost *cost*
no ip ospf cost

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

Interface cost reflects the port speed. This router uses a default cost of 1 for all ports. Therefore, if you install a Gigabit module, you may have to reset the cost for all of the 100 Mbps ports to a value greater than 1.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

Syntax

ip ospf dead-interval *seconds*
no ip ospf dead-interval

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

40, or four times the interval specified by the **ip ospf hello-interval** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

Related Commands

ip ospf hello-interval (4-361)

ip ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf hello-interval *seconds*
no ip ospf hello-interval

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

10 seconds

Command Usage

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

Syntax

ip ospf priority *priority*
no ip ospf priority

priority - Sets the interface priority for this router. (Range: 0-255)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

Syntax

ip ospf retransmit-interval *seconds*
no ip ospf retransmit-interval

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

5 seconds

Command Usage

A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

Syntax

ip ospf transmit-delay *seconds*
no ip ospf transmit-delay

seconds - Sets the estimated time required to send a link-state update. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1 second

Command Usage

LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links. The transmit delay must be the same for all routers attached to an autonomous system.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

show ip ospf

This command shows basic information about the routing configuration.

Command Mode

Privileged Exec

Example

```
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
     rip with metric mapped to 10
Number of area in this router is 2
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 19 times
Area 10.1.0.0
     Number of interfaces in this area is 4
     SPF algorithm executed 19 times
Console#
```

Table 4-88 show ip ospf - display description

Field	Description
Routing Process with ID	Router ID
Supports only single TOS (TOS0) route	Type of service is not supported, so you can only assign one cost per interface
It is an *router type*	The types displayed include internal, area border, or autonomous system boundary routers
Number of areas in this router	The number of configured areas
Area *identifier*	The area address, and area type if backbone, NSSA or stub
Number of interfaces	The number of interfaces attached to this area
SPF algorithm executed	The number of times the shortest path first algorithm has been executed for this area

show ip ospf border-routers

This command shows entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

Command Mode

Privileged Exec

Example

```
Console#show ip ospf border-routers

  Destination      Next Hop      Cost   Type  RteType      Area         SPF No
-------------- -------------- ------ ----- -------- --------------- -------
     10.1.1.252      10.1.1.253       0   ABR    INTRA         10.1.0.0        3
     10.2.6.252      10.2.9.253       0   ASBR   INTER         10.2.0.0        7
Console#
```

Table 4-89 show ip ospf border-routers - display description

Field	Description
Destination	Identifier for the destination router
Next Hop	IP address of the next hop toward the destination
Cost	Link metric for this route
Type	Router type of the destination; either ABR, ASBR or both
RteType	Route type; either intra-area or interarea route (INTRA or INTER)
Area	The area from which this route was learned
SPF No	The number of times the shortest path first algorithm has been executed for this route

show ip ospf database

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

Syntax

show ip ospf [*area-id*] **database** [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**database-summary**]

show ip ospf [*area-id*] **database** [**external**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**self-originate**] [*ip-address*]

show ip ospf [*area-id*] **database** [**network**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**router**] [*link-state-id*]
show ip ospf [*area-id*] **database** [[**router**] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**router**] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

- *area-id* - Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **adv-router** - IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- *ip-address* - IP address of the specified router. If no address is entered, information about the local router is displayed.
- **asbr-summary** - Shows information about Autonomous System Boundary Router summary LSAs.
- *link-state-id* - The network portion described by an LSA. The *link-state-id* entered should be:
  - An IP network number for Type 3 Summary and External LSAs

- A Router ID for Router, Network, and Type 4 AS Summary LSAs

Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).

- **self-originate** - Shows LSAs originated by this router.
- **database-summary** - Shows a count for each LSA type for each area stored in the database, and the total number of LSAs in the database.
- **external** - Shows information about external LSAs.
- **network** - Shows information about network LSAs.
- **nssa-external** - Shows information about NSSA external LSAs.
- **router** - Shows information about router LSAs.
- **summary** - Shows information about summary LSAs.

Command Mode

Privileged Exec

Examples

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database

     Displaying Router Link States(Area 10.1.0.0)
       Link ID      ADV Router    Age      Seq#     Checksum
--------------- --------------- ------ ---------- ----------
     10.1.1.252      10.1.1.252     26  0X80000005      0X89A1
     10.1.1.253      10.1.1.253     23  0X80000002      0X8D9D


     Displaying Net Link States(Area 10.1.0.0)
       Link ID      ADV Router    Age      Seq#     Checksum
--------------- --------------- ------ ---------- ----------
     10.1.1.252      10.1.1.252     28  0X80000001      0X53E1
Console#
```

Table 4-90 show ip ospf database - display description

Field	Description
Link ID	Router ID
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA

The following shows output when using the **asbr-summary** keyword.

```
Console#show ip ospf database asbr-summary

OSPF Router with id(10.1.1.253)

          Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 433
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 192.168.5.1 (AS Boundary Router's Router ID)
Advertising Router: 192.168.1.5
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0
Metric: 1

Console#
```

Table 4-91 show ip ospf asbr-summary - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to AS boundary routers
Link State ID	Interface address of the autonomous system boundary router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metrics	Cost of the link

The following shows output when using the **database-summary** keyword.

```
Console#show ip ospf database database-summary


Area ID (10.1.0.0)
       Router     Network     Sum-Net     Sum-ASBR     External-AS      External-Nssa
           2           1           1            0              0                0
Total LSA Counts : 4
Console#
```

Table 4-92 show ip ospf database-summary - display description

Field	Description
Area ID	Area identifier
Router	Number of router LSAs
Network	Number of network LSAs
Sum-Net	Number of summary LSAs
Sum-ASBR	Number of summary ASBR LSAs
External-AS	Number of autonomous system external LSAs
External-Nssa	Number of NSSA external network LSAs
Total LSA Counts	Total number of LSAs

The following shows output when using the **external** keyword.

```
Console#show ip ospf database external

OSPF Router with id(192.168.5.1) (Autonomous system 5)

          Displaying AS External Link States


LS age: 433
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.1.1.253 (External Network Number)
Advertising Router: 10.1.2.254
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0

Console#
```

Table 4-93 show ip ospf external - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS)
Link State ID	IP network number (External Network Number)
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metric Type	Type 1 or Type 2 external metric (see "redistribute" on page 4-347)
Metrics	Cost of the link
Forward Address	Forwarding address for data to be passed to the advertised destination (If set to 0.0.0.0, data is forwarded to the originator of the advertisement)
External Route Tag	32-bit field attached to each external route (Not used by OSPF; may be used to communicate other information between boundary routers as defined by specific applications)

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

OSPF Router with id(10.1.1.253)

          Displaying Net Link States(Area 10.1.0.0)


Link State Data Network (Type 2)
--------------------------------

LS age: 433
Options: Support External routing capability
LS Type: Network Links
Link State ID: 10.1.1.252 (IP interface address of the Designated
   Router)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0

       Attached Router: 10.1.1.252
       Attached Router: 10.1.1.253
Console#
```

Table 4-94 show ip ospf network - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Network Link - LSA describes the routers attached to the network
Link State ID	Interface address of the designated router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Attached Router	List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself

The following shows output when using the **router** keyword.

```
Console#show ip ospf database router

OSPF Router with id(10.1.1.253)

          Displaying Router Link States(Area 10.1.0.0)


Link State Data Router (Type 1)
-------------------------------

LS age: 233
Options: Support External routing capability
LS Type: Router Links
Link State ID: 10.1.1.252 (Originating Router's Router ID)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000011
LS Checksum: 0x7287
Length: 48
Router Role: Area Border Router
Number of Links: 1
-----------------------------------------------------
Link ID:  10.1.7.0 (IP Network/Subnet Number)
   Link Data: 255.255.255.0 (Network's IP address mask)
   Link Type: Connection to a stub network
   Number of TOS metrics: 0
   Metrics: 1

Console#
```

Table 4-95 show ip ospf router - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Router Link - LSA describes the router's interfaces.
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Router Role	Description of router type, including: None, AS Boundary Router, Area Border Router, or Virtual Link
Number of Links	Number of links described by the LSA
Link ID	Link type and corresponding Router ID or network address
Link Data	• Router ID for transit network • Network's IP address mask for stub network • Neighbor Router ID for virtual link
Link Type	Link-state type, including transit network, stub network, or virtual link
Number of TOS metrics	Type of Service metric – This router only supports TOS 0 (or normal service)
Metrics	Cost of the link

The following shows output when using the **summary** keyword.

```
Console#show ip ospf database summary

OSPF Router with id(10.1.1.253)

          Displaying Summary Net Link States(Area 10.1.0.0)


Link State Data Summary (Type 3)
--------------------------------

LS age: 686
Options: Support External routing capability
LS Type: Summary Links(Network)
Link State ID: 10.2.6.0 (The destination Summary Network Number)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000003
LS Checksum: 0x3D02
Length: 28
Network Mask: 255.255.255.0
Metric: 1

Console#
```

Table 4-96 show ip ospf summary - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to networks
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Destination network's IP address mask
Metrics	Cost of the link

show ip ospf interface

This command displays summary information for OSPF interfaces.

Syntax

show ip ospf interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Command Mode

Privileged Exec

Example

```
Console#show ip ospf interface vlan 1

Vlan 1 is up
  Interface Address 10.1.1.253, Mask 255.255.255.0, Area 10.1.0.0
  Router ID 10.1.1.253, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router id 10.1.1.252, Interface address 10.1.1.252
  Backup Designated router id 10.1.1.253, Interface addr 10.1.1.253
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Console#
```

Table 4-97 show ip ospf interface - display description

Field	Description
Vlan	VLAN ID and Status of physical link
Interface Address	IP address of OSPF interface
Mask	Network mask for interface address
Area	OSPF area to which this interface belongs
Router ID	Router ID
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)

Table 4-97 show ip ospf interface - display description (Continued)

Field	Description
State	• Disabled – OSPF not enabled on this interface • Down – OSPF is enabled on this interface, but interface is down • Loopback – This is a loopback interface • Waiting – Router is trying to find the DR and BDR • DR – Designated Router • BDR – Backup Designated Router • DRother – Interface is on a multiaccess network, but is not the DR or BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

show ip ospf neighbor

This command displays information about neighboring routers on each interface within an OSPF area.

Syntax

show ip ospf neighbor

Command Mode

Privileged Exec

Example

```
Console#show ip ospf neighbor

      ID          Pri         State          Address
--------------- ------ ---------------- ---------------
     10.1.1.252      1          FULL/DR      10.1.1.252

Console#
```

Table 4-98 show ip ospf neighbor - display description

Field	Description
ID	Neighbor's router ID
Pri	Neighbor's router priority
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Address	IP address of this interface

show ip ospf summary-address

This command displays all summary address information.

Syntax

show ip ospf summary-address

Command Mode

Privileged Exec

Example

This example shows a summary address and associated network mask.

```
Console#show ip ospf summary-address
10.1.0.0/255.255.0.0
Console#
```

Related Commands

summary-address (4-346)

show ip ospf virtual-links

This command displays detailed information about virtual links.

Syntax

show ip ospf virtual-links

Command Mode

Privileged Exec

Example

```
Console#show ip ospf virtual-links
Virtual Link to router 10.1.1.253 is up
Transit area 10.1.1.0
Transmit Delay is 1 sec
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Console#
```

Table 4-99 show ip ospf virtual-links - display description

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

Related Commands

area virtual-link (4-353)

Multicast Routing Commands

This router uses IGMP snooping and query to determine the ports connected to downstream multicast hosts, and to propagate this information back up through the multicast tree to ensure that requested services are forwarded through each intermediate node between the multicast server and its hosts, and also to filter traffic from all of the other interfaces that do not require these services.

Static Multicast Routing Commands

Table 4-100 Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	4-379
show ip igmp snooping mrouter	Shows multicast router ports	PE	4-380

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-25/49)
  - **port-channel** *channel-id* (Range: 1-32)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
Console#
```

Router Redundancy Commands

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Table 4-101 Router Redundancy Commands

Command Groups	Function	Page
Virtual Router Redundancy Protocol	Configures interface settings for VRRP	4-381

Virtual Router Redundancy Protocol Commands

To configure VRRP, select an interface on one router in the group to serve as the master virtual router. This physical interface is used as the virtual address for the router group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line.

Table 4-102 VRRP Commands

Command	Function	Mode	Page
vrrp ip	Enables VRRP and sets the IP address of the virtual router	IC	4-382
vrrp authentication key	Configures a key used to authenticate VRRP packets received from other routers	IC	4-383
vrrp priority	Sets the priority of this router in the VRRP group	IC	4-384
vrrp timers advertise	Sets the interval between successive advertisements by the master virtual router	IC	4-385
vrrp preempt	Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router	IC	4-386
show vrrp	Displays VRRP status information	PE	4-387

Table 4-102 VRRP Commands (Continued)

Command	Function	Mode	Page
show vrrp interface	Displays VRRP status information for the specified interface	PE	4-389
show vrrp router counters	Displays VRRP statistics	PE	4-390
show vrrp interface counters	Displays VRRP statistics for the specified interface	PE	4-391
clear vrrp router counters	Clears VRRP router statistics	PE	4-391
clear vrrp interface counters	Clears VRRP interface statistics	PE	4-392

vrrp ip

This command enables the Virtual Router Redundancy Protocol (VRRP) on an interface and specify the IP address of the virtual router. Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

Syntax

[**no**] **vrrp** *group* **ip** *ip-address* [**secondary**]

- *group* - Identifies the virtual router group. (Range: 1-255)
- *ip-address* - The IP address of the virtual router.
- **secondary** - Specifies additional secondary IP addresses assigned to the current VLAN interface that are supported by this VRRP group.

Default Setting

No virtual router groups are configured.

Command Mode

Interface (VLAN)

Command Usage

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.

- The IP address assigned to the virtual router must already be configured on the router that will be the Owner. In other words, the IP address specified in this command must already exist on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.
- If you have multiple secondary addresses configured on the current VLAN interface, you can use this command with the **secondary** keyword to add any secondary address that will be supported by the virtual router.
- VRRP is enabled as soon as this command is entered. If you need to customize any of the other parameters for VRRP such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

Example

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner, and also adds a secondary interface as a member of the group.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#vrrp 1 ip 192.168.2.6 secondary
Console(config-if)#
```

vrrp authentication

This command specifies the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

Syntax

vrrp *group* **authentication** *key*
no vrrp *group* **authentication**

- *group* - Identifies the virtual router group. (Range: 1-255)
- *key* - Authentication string. (Range: 1-8 alphanumeric characters)

Default Setting

No key is defined.

Command Mode

Interface (VLAN)

Command Usage

- All routers in the same VRRP group must be configured with the same authentication key.
- When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.
- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

Example

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp priority

This command sets the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

Syntax

vrrp *group* **priority** *level*
no vrrp *group* **priority**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *level* - Priority of this router in the VRRP group. (Range: 1-254)

Default Setting

100

Command Mode

Interface (VLAN)

Command Usage

- A router that has a physical interface with the same IP address as that used for the virtual router will become the master virtual router. The

backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.

- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.
- If the backup preempt function is enabled with the **vrrp preempt** command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.

Example

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

Related Commands

vrrp preempt (4-386)

vrrp timers advertise

This command sets the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

Syntax

vrrp *group* **timers advertise** *interval*
no vrrp *group* **timers advertise**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *interval* - Advertisement interval for the master virtual router. (Range: 1-255 seconds)

Default Setting

1 second

Command Mode

Interface (VLAN)

Command Usage

- VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
- VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated VRRP group.
- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second

Example

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

vrrp preempt

This command configures the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

Syntax

vrrp *group* **preempt** [**delay** *seconds*]
no vrrp *group* **preempt**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *seconds* - The time to wait before issuing a claim to become the master. (Range: 0-120 seconds)

Default Setting

- Preempt: Enabled
- Delay: 0 seconds

Command Mode

Interface (VLAN)

Command Usage

- If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However,

note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.

- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

Example

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

Related Commands

vrrp priority (4-384)

show vrrp

This command displays status information for VRRP.

Syntax

show vrrp [**brief** | *group*]

- **brief** - Displays summary information for all VRRP groups on this router.
- *group* - Identifies a VRRP group. (Range: 1-255)

Defaults

None

Command Mode

Privileged Exec

Command Usage

- Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- Specify a group number to display status information for a specific group

Example

This example displays the full listing of status information for all groups.

```
Console#show vrrp
 Vlan 1 - Group 1,
 state                          Master
 Virtual IP address             192.168.1.6
 Virtual MAC address            00-00-5E-00-01-01
 Advertisement interval         5 sec
 Preemption                     enabled
 Min delay                      10 sec
 Priority                       1
 Authentication                 SimpleText
 Authentication key             bluebird
 Master Router                  192.168.1.6
 Master priority                255
 Master Advertisement interval  5 sec
 Master down interval           15
Console#
```

Table 4-103 show vrrp - display description

Field	Description
State	VRRP role of this interface (master or backup)
Virtual IP address	Virtual address that identifies this VRRP group
Virtual MAC address	Virtual MAC address derived from the owner of the virtual IP address
Advertisement interval	Interval at which the master virtual router advertises its role as the master
Preemption	Shows whether or not a higher priority router can preempt the current acting master
Min delay	Delay before a router with a higher priority can preempt the current acting master
Priority	Priority of this router
Authentication	Authentication mode used to verify VRRP packets
Authentication key	Key used to authenticate VRRP packets received from other routers
Master Router	IP address of the router currently acting as the VRRP group master
Master priority	The priority of the router currently acting as the VRRP group master

Table 4-103 show vrrp - display description (Continued)

Field	Description
Master Advertisement interval	The advertisement interval configured on the VRRP master.
Master down interval	The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings)

This example displays the brief listing of status information for all groups.

```
Console#show vrrp brief
Interface   Grp    State    Virtual addr     Int   Pre   Prio
-------------------------------------------------------------
vlan 1      1      Master   192.168.1.6      5      E    1
Console#
```

Table 4-104 show vrrp brief - display description

Field	Description
Interface	VLAN interface
Grp	VRRP group
State	VRRP role of this interface (master or backup)
Virtual addr	Virtual address that identifies this VRRP group
Int	Interval at which the master virtual router advertises its role as the master
Pre	Shows whether or not a higher priority router can preempt the current acting master
Prio	Priority of this router

show vrrp interface

This command displays status information for the specified VRRP interface.

Syntax

show vrrp interface vlan *vlan-id* [**brief**]

- *vlan-id* - Identifier of configured VLAN interface. (Range: 1-4093)
- **brief** - Displays summary information for all VRRP groups on this router.

Defaults

None

Command Mode

Privileged Exec

Example

This example displays the full listing of status information for VLAN 1.

```
Console#show vrrp interface vlan 1
 Vlan 1 - Group 1,
 state                              Master
 Virtual IP address                 192.168.1.6
 Virtual MAC address                00-00-5E-00-01-01
 Advertisement interval             5 sec
 Preemption                         enabled
 Min delay                          10 sec
 Priority                           1
 Authentication                     SimpleText
 Authentication key                 bluebird
 Master Router                      192.168.1.6
 Master priority                    1
 Master Advertisement interval      5 sec
 Master down interval               15
Console#
```

* Refer to "show vrrp" on page 4-387 for a description of the display items.

show vrrp router counters

This command displays counters for errors found in VRRP protocol packets.

Command Mode

Privileged Exec

Example

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```
Console#show vrrp router counters
 Total Number of VRRP Packets with Invalid Checksum : 0
 Total Number of VRRP Packets with Unknown Error    : 0
 Total Number of VRRP Packets with Invalid VRID     : 0
Console#
```

show vrrp interface counters

This command displays counters for VRRP protocol events and errors that have occurred for the specified group and interface.

show vrrp *group* **interface vlan** *interface* **counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4093)

Defaults

None

Command Mode

Privileged Exec

Example

```
Console#show vrrp 1 interface vlan 1 counters
 Total Number of Times Transitioned to MASTER                       : 6
 Total Number of Received Advertisements Packets                    : 0
 Total Number of Received Error Advertisement Interval Packets      : 0
 Total Number of Received Authentication Failures Packets           : 0
 Total Number of Received Error IP TTL VRRP Packets                 : 0
 Total Number of Received Priority 0 VRRP Packets                   : 0
 Total Number of Sent Priority 0 VRRP Packets                       : 5
 Total Number of Received Invalid Type VRRP Packets                 : 0
 Total Number of Received Error Address List VRRP Packets           : 0
 Total Number of Received Invalid Authentication Type VRRP Packets  : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets : 0
 Total Number of Received Error Packet Length VRRP Packets          : 0
Console#
```

* Refer to "Displaying VRRP Group Statistics" on page 3-263 for a description of the display items.

clear vrrp router counters

This command clears VRRP system statistics.

Command Mode

Privileged Exec

Example

```
Console#clear vrrp router counters
Console#
```

clear vrrp interface counters

This command clears VRRP system statistics for the specified group and interface.

clear vrrp *group* **interface** *interface* **counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4093)

Defaults

None

Command Mode

Privileged Exec

Example

```
Console#clear vrrp 1 interface 1 counters
Console#
```

APPENDIX A
SOFTWARE SPECIFICATIONS

Software Features

Authentication
Local, RADIUS, TACACS, Port (802.1X), HTTPS, SSH, Port Security

Access Control Lists
IP, MAC (up to 32 lists)

DHCP Client, Relay, Server

DNS Server

Port Configuration
1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex
1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP),
10GBASE-LR - 10 Gbps at full duplex (Module)

Broadcast Storm Control
Traffic throttled above a critical threshold

Port Mirroring
Multiple source ports, one destination port

Rate Limits
Input Limit
Output limit
Range (configured per port)

Port Trunking
Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Algorithm
Spanning Tree Protocol (STP, IEEE 802.1D)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)
Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s)

VLAN Support
Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),
GVRP for automatic VLAN learning, private VLANs

Class of Service
Supports eight levels of priority and Weighted Round Robin Queueing (which can be configured by VLAN tag or port),
Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

Quality of Service
DiffServ supports class maps, policy maps, and service policies

Multicast Filtering
IGMP Snooping (Layer 2)

IP Routing
ARP, Proxy ARP
Static routes
RIP, RIPv2 and OSPFv2 dynamic routing
VRRP (Virtual Router Redundancy Protocol)

Additional Features
BOOTP client
CIDR (Classless Inter-Domain Routing)
SNTP (Simple Network Time Protocol)
SNMP (Simple Network Management Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts

Management Features

In-Band Management
Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management
RS-232 DB-9 console port

Software Loading
TFTP in-band or XModem out-of-band

SNMP
Management access via MIB database
Trap management to specified hosts

RMON
Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1s Multiple Spanning Tree Protocol
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1X Port Authentication
IEEE 802.3-2002
  Ethernet, Fast Ethernet, Gigabit Ethernet
  Link Aggregation Control Protocol (LACP)
IEEE 802.3ac VLAN tagging
ARP (RFC 826)
DHCP Client (RFC 1541)
DHCP Relay (RFC 951)
DHCP Server (RFC 2131)
HTTPS

ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
OSPF (RFC 2328, 1587)
RADIUS+ (RFC 2618)
RIP (RFC 1058)
RIPv2 (RFC 2453)
RMON (RFC 1757 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 2571)
SNMPv3 (RFC RAFT 3414, 2570, 2273, 3411, 3415)
SNTP (RFC 2030)
SSH (Version 2.0)
TFTP (RFC 1350)
VRRP (RFC 2338)

Management Information Bases

Bridge MIB (RFC 1493)
DNS Resolver MIB (RFC 1612)
DVMRP MIB
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
IP Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
MAU MIB (RFC 2668)
MIB II (RFC 1213)
OSPF MIB (RFC 1850)
Port Access Entity MIB (IEEE 802.1X)

Port Access Entity Equipment MIB
Private MIB
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
RIP1 MIB (RFC 1058)
RIP2 MIB (RFC 2453)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMPv2 IP MIB (RFC 2011)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMP Community MIB (RFC 2576)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2013)
Trap (RFC 1215)
UDP MIB (RFC 2012)
VRRP MIB (RFC 2787)

APPENDIX B
TROUBLESHOOTING

Problems Accessing the Management Interface

Table B-1 Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	• Be sure the switch is powered up. • Check network cabling between the management station and the switch. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.

Table B-1 Troubleshooting Chart

Symptom	Action
Cannot connect using Secure Shell	• If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. • Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. • Be sure you have generated a public key on the switch, and exported this key to the SSH client. • Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. • Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact your local distributor.

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Designate the SNMP host that is to receive the error messages.
4. Repeat the sequence of commands or other actions that lead up to the error.
5. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
6. Contact your distributor's service engineer.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
:
```

GLOSSARY

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services (DiffServ)

DiffServ provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be

marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories

by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message-Digest Algorithm

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in

order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1X.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Quality of Service (QoS)

QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Algorithm (STA)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical

barriers, and allows users to share information and resources as though located on the same LAN.

Virtual Router Redundancy Protocol (VRRP)

A protocol that uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

INDEX

Numerics

802.1X, port authentication 3-93, 4-104

A

acceptable frame type 3-194, 4-251
Access Control List *See* ACL
ACL
  Extended IP 3-104, 4-114, 4-116, 4-119
  MAC 3-104, 4-114, 4-128, 4-129–4-132
  Standard IP 3-104, 4-114, 4-116, 4-118
Address Resolution Protocol *See* ARP
address table 3-151, 4-216
  aging time 3-155, 4-220
ARP
  configuration 3-274, 4-313
  description 3-273
  proxy 3-274, 4-316
  statistics 3-280, 4-323

B

BOOTP 3-25, 4-308
BPDU 3-156
broadcast storm, threshold 3-140, 4-194

C

Class of Service *See* CoS
CLI, showing commands 4-4
command line interface *See* CLI
community string 2-13, 3-53, 4-141
configuration settings, saving or restoring 2-15, 3-30, 4-84
console port, required connections 2-3
CoS
  configuring 3-203, 4-269, 4-284
  DSCP 3-212, 4-279
  IP port priority 3-214, 4-276
  IP precedence 3-210, 4-278
  layer 3/4 priorities 3-209, 4-276
  queue mapping 3-205, 4-273
  queue mode 3-207, 4-270
  traffic class weights 3-208, 4-272

D

default gateway, configuration 3-23, 3-269, 4-310
default priority, ingress port 3-203, 4-271
default settings, system 1-9
DHCP 3-25, 4-308
  address pool 3-246, 4-163
  client 3-23, 4-157, 4-177
  dynamic configuration 2-11
  relay service 3-242, 4-159
  server 3-244, 4-161
Differentiated Code Point Service *See* DSCP
Differentiated Services *See* DiffServ
DiffServ 3-217, 4-284
  binding policy to interface 3-225, 4-293
  class map 3-218, 4-286, 4-290
  policy map 3-221, 4-289
  service policy 3-225, 4-293
DNS
  default domain name 3-235, 4-179
  displaying the cache 3-240
  domain name list 3-235, 4-178
  enabling lookup 3-235, 4-182
  name server list 3-235, 4-181
  static entries 3-238
Domain Name Service *See* DNS

downloading software 3-28, 4-84
DSCP
  enabling 3-210, 4-279
  mapping priorities 3-212, 4-280
dynamic addresses, displaying 3-153, 4-219
Dynamic Host Configuration Protocol *See* DHCP

E

edge port, STA 3-169, 3-172, 4-237
event logging 4-57

F

firmware
  displaying version 3-17, 4-81
  upgrading 3-28, 4-84

G

GARP VLAN Registration Protocol *See* GVRP
gateway, default 3-23, 3-270, 4-310
GVRP
  global setting 3-185, 4-264
  interface configuration 3-195, 4-266

H

hardware version, displaying 3-17, 4-81
HTTPS 3-80, 4-42
HTTPS, secure server 3-80, 4-42

I

IEEE 802.1D 3-156, 4-223
IEEE 802.1s 4-223
IEEE 802.1w 3-156, 4-223
IEEE 802.1X 3-93, 4-104
IGMP
  groups, displaying 3-232, 4-299
  Layer 2 3-227, 4-296
  query 3-227, 4-301
  query, Layer 2 3-228, 4-300
  snooping 3-227, 4-297
  snooping, configuring 3-228, 4-296
ingress filtering 3-194, 4-252
IP address
  BOOTP/DHCP 3-25, 4-158, 4-308
  setting 2-10, 3-22, 4-308
IP port priority
  enabling 3-214, 4-276
  mapping priorities 3-214, 4-277
IP precedence
  enabling 3-210, 4-278
  mapping priorities 3-210, 4-278
IP routing 3-265, 4-317
  configuring interfaces 3-271, 4-308
  enabling or disabling 3-269, 4-318
  status 3-270, 4-318
  unicast protocols 3-268
IP, statistics 3-282, 4-323

J

jumbo frame 4-82

L

LACP
  configuration 4-204
  local parameters 3-135, 4-212
  partner parameters 3-138, 4-212
  protocol message statistics 4-212
  protocol parameters 3-130, 4-204
Link Aggregation Control Protocol *See* LACP
link type, STA 3-169, 3-172, 4-239

logging
  syslog traps 4-61
  to syslog servers 4-60
log-in, Web interface 3-3
logon authentication 3-74, 4-91
  RADIUS client 3-76, 4-94
  RADIUS server 3-76, 4-94
  TACACS+ client 3-77, 4-99
  TACACS+ server 3-77, 4-99
logon authentication, sequence 3-78, 4-92, 4-93

M

main menu 3-5
Management Information Bases (MIBs) A-4
mirror port, configuring 3-142, 4-200
MSTP 4-223
  global settings 3-173, 4-221
  interface settings 3-170, 4-222
multicast filtering 3-226, 4-296
multicast groups 3-232, 4-299
  displaying 4-299
  static 3-232, 4-297, 4-299
multicast routing 4-379
multicast services
  configuring 3-233, 4-297
  displaying 3-232, 4-299
multicast, static router port 3-231, 4-305, 4-379

O

OSPF 3-303, 4-338
  area border router 3-306, 4-344
  AS summary route 3-325, 4-346
  autonomous system boundary router 3-306, 4-342
  backbone 3-309, 4-349
  default external route 3-307, 4-342
  general settings 3-305, 4-338
  normal area 3-309, 4-348
  NSSA 3-309, 4-351
  redistributing external routes 3-327, 4-347
  stub 3-309, 4-350
  transit area 3-309, 4-353
  virtual link 3-321, 4-353

P

password, line 4-17
passwords 2-9
  administrator setting 3-75, 4-35
path cost 3-158, 3-168
  method 3-164, 4-228
  STA 3-158, 3-168, 4-228
port authentication 3-93, 4-104
port priority
  configuring 3-203, 4-269, 4-284
  default ingress 3-203, 4-271
  STA 3-168, 4-236
port security, configuring 3-90, 4-101
port, statistics 3-145, 4-197
ports
  autonegotiation 3-122, 4-189
  broadcast storm threshold 3-140, 4-194
  capabilities 3-122, 4-190
  duplex mode 3-122, 4-188
  forced selection on combo ports 4-192
  speed 3-122, 4-188
ports, configuring 3-119, 4-186
ports, mirroring 3-142, 4-200
priority, default port ingress 3-203, 4-271
problems, troubleshooting B-1
protocol migration 3-172, 4-242
proxy ARP 3-274, 4-316

Q

QoS 3-216, 4-284
Quality of Service *See* QoS
queue weights 3-208, 4-272

R

RADIUS, logon authentication 3-76, 4-94
rate limits, setting 3-144, 4-203
remote logging 4-61
restarting the system 3-47, 4-30
RIP
  configuring 3-292, 4-325—4-336
  description 3-268
  global settings 3-293, 4-325
  interface protocol settings 3-296, 4-327—4-334
  specifying interfaces 3-295, 4-327
  statistics 3-300, 4-337
router redundancy
  protocols 3-254, 4-381
  VRRP 3-256, 4-381
routing table, displaying 3-290, 4-320, 4-322
RSTP 3-155, 4-223
  global configuration 3-157, 4-223

S

secure shell 3-83, 4-45
Secure Shell configuration 3-83, 4-49, 4-50
serial port
  configuring 4-14
SNMP 3-50
  community string 3-53, 4-141
  enabling traps 3-54, 4-146
  trap manager 3-54, 4-143
software
  displaying version 3-17, 4-81
  downloading 3-28, 4-84
Spanning Tree Protocol *See* STA
specifications, software A-1
SSH, configuring 3-83, 4-49, 4-50
STA 3-155, 4-221
  edge port 3-169, 3-172, 4-237
  global settings, configuring 3-161, 4-222—4-229
  global settings, displaying 3-157, 4-243
  interface settings 3-166, 3-177, 3-179, 4-235—4-242, 4-243
  link type 3-169, 3-172, 4-239
  path cost 3-158, 3-168, 4-235
  path cost method 3-164, 4-228
  port priority 3-168, 4-236
  protocol migration 3-172, 4-242
  transmission limit 3-164, 4-229
standards, IEEE A-3
startup files
  creating 3-32, 4-84
  displaying 3-28, 4-76
  setting 3-28, 4-90
static addresses, setting 3-151, 4-217
static routes, configuring 3-289, 4-319
statistics
  ARP 3-280, 4-323
  ICMP 3-284, 4-323
  IP 3-282, 4-323
  port 3-145, 4-197
  RIP 3-300, 4-337
  TCP 3-288, 4-323
  UDP 3-287, 4-323
STP 3-162, 4-223
STP *Also see* STA
system clock, setting 3-48, 4-69
system software, downloading from server 3-28, 4-84

T

TACACS+, logon authentication 3-77, 4-99
time, setting 3-48, 4-69
traffic class weights 3-208, 4-272
trap manager 2-14, 3-54, 4-143
troubleshooting B-1
trunk
  configuration 3-125, 4-204
  LACP 3-128, 4-204, 4-206
  static 3-126, 4-206

U

upgrading software 3-28, 4-84
user account 3-75
user password 3-75, 4-35, 4-37

V

Virtual Router Redundancy Protocol *See* VRRP
VLANs 3-181—3-198, 4-245—4-258
  adding static members 3-190, 3-193, 4-254
  creating 3-188, 4-247
  description 3-181
  displaying basic information 3-186, 4-265
  displaying port members 3-187, 4-256
  egress mode 3-195, 4-250
  interface configuration 3-194, 4-251—4-255
  private 3-197, 4-257
  protocol 3-199, 4-259
VRRP 3-256, 4-381
  authentication 3-259, 4-383
  configuration settings 3-256, 4-381
  group statistics 3-263, 4-387
  preemption 3-257, 3-258, 4-386
  priority 3-257, 3-259, 4-384
  protocol message statistics 3-262, 4-390
  timers 3-258, 4-385
  virtual address 3-256, 3-258, 4-382

W

Web interface
  access requirements 3-1
  configuration buttons 3-4
  home page 3-3
  menu list 3-5
  panel display 3-4

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481
From Europe: Contact details can be found on
www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
World Wide Web:
http://www.smc.com
http://www.smc-europe.com

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-91-352-00-40;	Fax 34-93-477-3774
UK:	44 (0) 1932 866553;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 335 5708602;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	216-712-36616;	Fax 216-71751415
North West Africa:	34 93 477 4920;	Fax 34 93 477 3774
CIS:	7 (095) 7893573;	Fax 7 (095) 789 35 73
PRC:	86-10-6235-4958;	Fax 86-10-6235-4962
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 238 6556;	Fax (65) 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-45-224-2332;	Fax 81-45-224-2331
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91-22-8204437;	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com, www.smc-europe.com, or www.smc-asia.com.

SMC® Networks

38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC8724ML3/SMC8748ML3
Pub. Number: 149100023600A
Revision Number: F1.0.0.0 E062005-R02